DETERMINAR EL NIVEL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL INSTITUTO MUSEO NACIONAL (IMN)

EDDIE LUIS RADA GONZÁLEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CEAD BARRANQUILLA
BOGOTÁ
2017

DETERMINAR EL NIVEL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL INSTITUTO MUSEO NACIONAL (IMN)

EDDIE LUIS RADA GONZÁLEZ
72018801

Monografía para optar el Título de Especialista en Seguridad Informática

Ingeniera: Erika Liliana Villamizar Torres
Directora

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA.
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CEAD BARRANQUILLA
2017

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá, 22 de julio de 2017

DEDICATORIA

Dedico este proyecto de grado al Padre Eterno como toda la energía creadora de Luz, especialmente a mis padres, hermanas, hija, novia y a todas aquellas personas que me han aportado en mi aprendizaje de forma positiva y superación profesional.

AGRADECIMIENTOS

A mis padres por el apoyo y motivación contaste y el gran ejemplo a seguir en esta especialización, la cual es de mucha importancia para mi vida profesional, a mis hermanas y compañeros de estudio y trabajo, de igual manera agradecer al director del curso y todos los tutores que me han colaborado con todo el apoyo el amor y la paciencia que han tenido en mí proceso de aprendizaje.

CONTENIDO

pág.

LISTA DE ANEXOS

pág.

LISTA DE TABLAS

pág.

LISTA DE GRÁFICAS

pág.

LISTA DE FIGURAS

pág.

GLOSARIO

ACTIVO: es un recurso, proceso, producto o sistema que tiene algún valor para la organización y por lo tanto debe ser protegido.

AMENAZAS: cualquier circunstancia natural o hecha por el hombre o evento que pueda tener un impacto adverso o no deseado, menor o mayor sobre una organización. Es una causa potencial de un incidente no deseado la cual puede terminar en el daño o la denegación del sistema de la organización.

CONFIDENCIALIDAD: evitar el uso no autorizado ó la divulgación de información, asegurando que la información es únicamente accedida por aquellos autorizados a tener acceso a ella. Privacidad es un concepto cerrado que está relacionado con la información personal, la Privacidad asegura la confidencialidad de los datos personales.

DISPONIBILIDAD: asegura que los usuarios autorizados tengan confiable y rápido acceso a la información y activos asociados cuando sea requerido.

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: es una ocurrencia identificada de un sistema, servicio, o estado de la red indicando un posible rompimiento de la política de seguridad de información o falla de garantías, o previamente una situación no conocida que puede ser relevante a seguridad.

EXPLOIT: es el nombre dado a los programas que hacen uso de los errores o bugs de las aplicaciones o sistemas, los cuales pertenecen a alguien externo que causa que este realice algo para lo cual no fue creado. Código escrito con el fin de aprovechar un error de programación para obtener diversos privilegios, software o explotar una vulnerabilidad.

VULNERABILIDAD: es cualquier defecto o falla que un atacante puede utilizar para ganar acceso a un sistema o la red. Es una debilidad de un activo o un grupo de activos que puede ser explotada por una amenaza.

POLÍTICAS: una política de seguridad forma la base del programa de seguridad de la información de las organizaciones. Son declaraciones formales de reglas que deben ser acatadas por las personas que tienen acceso a la tecnología de la organización y a los activos de información.

PHISHING: es una forma de actividad criminal que usa técnicas de ingeniería social, caracterizado por intentar adquirir de forma fraudulenta información sensible como passwords y detalles de tarjetas de crédito. Una forma de lograrlo es hacerse pasar por personas confiables o enviando mensajes de negocio con la apariencia de una comunicación electrónica oficial utilizando e- mail ó mensajería instantánea. El

término surge de usar sofisticados señuelos para pescar información financiera de usuarios y passwords.

RIESGO: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y su consecuencia.

SEGURIDAD DE LA INFORMACIÓN: preservación de la confidencialidad, integridad y disponibilidad de la información en adición a otras propiedades tales como, autenticidad, contabilidad, no repudiación y la fiabilidad también puede ser incluido.

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: es indicado por uno o varios eventos de seguridad de la información no deseada o no esperada que tienen una significativa probabilidad de comprometer la operación del negocio y el tratamiento de la seguridad de la información.

INTEGRIDAD: certificar la exactitud y totalidad de la información y los métodos de procesamiento, Esto asegura que modificaciones a los datos no sean hechos por usuarios ó procesos no autorizados. Los datos son interna y externamente consistente, dicho en otras palabras, para una entrada dada hay una salida esperada.

RESUMEN

El cuidado de la información debe tener una importancia fundamental para el funcionamiento e inclusive para que el instituto logre en el corto, mediano y largo plazo la consecución de su misión y además garantiza su supervivencia en un entorno cada vez más dinámico y lleno de riesgos. El hecho de disponer de una serie de controles para mitigar el riesgo según NTC/ISO 27001:2013 ayuda a gestionar y proteger los valiosos activos de información; activos indispensables para la operación y funcionamiento de los procesos misionales.

Este proyecto básicamente está organizado en cuatro (4) fases las cuales están estrechamente relacionadas con la norma NTC/ISO 27001:2013 y el Modelo de Seguridad Y Privacidad de La Información – MPSI de la Estrategia de Gobierno en Línea - GEL. Estos modelos han sido establecidos para ofrecer una guía para el establecimiento, implementación, operación, seguimiento, revisión y mejora de un Sistema de Gestión de la Seguridad de la Información (SGSI). La adopción de este sistema es una decisión de tipo estratégico. El diseño y la posterior implementación del SGSI, deben estar basados en el tamaño, la estructura, las necesidades, los objetivos y los procesos del Instituto.

En la parte inicial de este proyecto se realizó el levantamiento de la información para la identificación de los activos de información, luego se analizaron sus riesgos y amenazas, finalmente se realizaron pruebas de vulnerabilidades para determinar las brechas de seguridad para la cual se recomiendan algunos procedimientos y procesos mitigando así el mayor número riesgos y amenazas posibles para el instituto.

PALABRAS CLAVES: Activo, Amenazas, Confidencialidad, Diagnostico, Disponibilidad, Integridad, Políticas, Pruebas, Riesgo, Vulnerabilidad.

INTRODUCCIÓN

El IMN (Instituto Museo Nacional), de acuerdo con los propósitos definidos en el Manual Gobierno en Línea en su versión más reciente para los establecimientos públicos del orden nacional, específicamente en lo relacionado con el componente de Seguridad y Privacidad de la Información y dando cumplimiento a lo establecido en el decreto 2573 de 2014 , ha decidido implementar un Sistema de Gestión de Seguridad de la Información (SGSI) el cual tendrá como alcance el proceso misional Gestión de Formación Profesional Integral.

En el marco de dicha implementación, y obedeciendo lo definido en el criterio Diagnóstico de Seguridad y Privacidad de la información del instituto ya mencionado, el IMN ha solicitado la realización de Pruebas de Análisis de Vulnerabilidades sobre las tecnologías de información y comunicaciones a los procesos a los cuales se está ejecutando el SGSI.

El interés de la ejecución del proyecto con la entrega del presente documento es el de presentar los resultados de las pruebas de “Análisis de Vulnerabilidades”, desarrollar las recomendaciones, pero, ante todo, disminuir al máximo cualquier riesgo que se pueda derivar de la ejecución de las actividades propias de las pruebas y que eventualmente pudiera generar un impacto negativo en la operación del IMN, ayudando a la reducción de costos operativos y financieros, estableciendo una cultura de seguridad y garantizando el cumplimiento de los requerimientos legales, contractuales y procesos administrativos.

El desarrollo se realiza bajo la gestión del grupo de especialistas en seguridad informática, designados por parte de los directivos del Instituto para elaboración de los documentos solicitados en la gestión documental del SGSI, bajo la normativa ISO/IEC 27001:2013 para la administración de la tecnología estableciendo los roles y responsabilidades dentro de los procesos como calidad, riesgos, continuidad y seguridad y verificación de la información.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Realizar un diagnóstico para determinar el nivel de seguridad y privacidad de la información del INSTITUTO MUSEO NACIONAL (IMN) conforme a la norma ISO 27001:2013

1.2 OBJETIVOS ESPECÍFICOS

- Realizar el levantamiento de la información mediante el análisis Gap, con respecto a la seguridad y privacidad de la información al interior del Instituto basado en la norma ISO 27001:2013.

- Identificar y clasificar los activos de información del instituto, mediante procedimientos, y metodologías propuestas.

- Realizar el informe de la evaluación de riesgos de seguridad para determinar los procedimientos y mapas de riesgo que puedan afectar la confidencialidad, la integridad y la disponibilidad de la información del instituto.

- Ejecutar las pruebas de hacking ético y presentar los resultados con el respectivo análisis y recomendaciones para mitigar las vulnerabilidades encontradas en los activos de información críticos.

2. ALCANCE

El presente proyecto está fundamentado en la realización de la fase del diagnóstico de seguridad y privacidad de la información del Instituto Museo Nacional - IMN, como proyecto investigativo y simulación con un tipo de estudio basado en el enfoque educativo, dicho diagnóstico corresponde a la primera fase para una futura implementación del modelo de seguridad y privacidad de la información del INSTITUTO MUSEO NACIONAL (IMN) conforme a la norma ISO 27001:2013

Este diagnóstico se aplicará exclusivamente a la oficina de tecnologías de la información del IMN, debido a que realiza procesos misionales y transversales a todos los que se llevan actualmente en el instituto.

3. PLANTEAMIENTO DEL PROBLEMA

El Instituto Museo Nacional – IMN como muchas otras entidades del estado, ejecutan gran parte de su presupuesto y esfuerzo para brindar la seguridad apropiada a sus activos de información como el insumo para la toma de decisiones. El brindar seguridad en la información no es solamente la implementación de un Antivirus, Anti spam o un Firewall en la red. Si no que va mucho más allá, y debe ir bajo los Lineamientos institucionales, políticas vigentes y las directrices del Ministerio de las Tics y los demás entes que puedan intervenir.

A pesar de haber algunas políticas de seguridad informática y controles con formatos establecidos, el instituto en la actualidad no cuenta con un diagnostico el cual determine el nivel de seguridad y privacidad de la información, donde se evalúen y se realice un control y seguimiento a los temas críticos de seguridad en las diferentes áreas donde se pueda asegurar la continuidad del negocio, minimizar los daños y maximizar el retorno de las inversiones.

¿Un diagnostico a la seguridad y privacidad de la información le proporcionará al Instituto IMN los mecanismos, elementos y lineamientos para el diseño e implementación del modelo de seguridad y privacidad de la información MSPI como parte del sistema de gestión de la seguridad de la información SGSI.?

4. JUSTIFICACIÓN

Tanto para el INSTITUTO MUSEO NACIONAL (IMN), como para otras entidades públicas en el estado colombiano, la seguridad de la información en sus etapas tempranas se ha centrado en la protección de la tecnología de la información orientada a servicio de procesamiento y almacenamiento, más que a la información en sí misma, que es a lo que se le denomina seguridad informática.

Para el caso del Instituto IMN es necesario extender el alcance centrado en la tecnología y apuntar a una seguridad integral, en la que se proteja la información sin importar cómo se maneja, se procesa o se almacena. El "Diagnostico al Modelo de seguridad y Privacidad de la información - MPSI" Es la primera etapa previa a la implementación dentro del marco de seguridad, con la cual se pretende realizar un análisis bajo los lineamientos de la estrategia de gobierno en Línea - GEL, liderada por El Ministerio de Tecnologías de la información y las comunicaciones. Por lo tanto, esta primera etapa es de vital importancia como base primordial para poder garantizar mínimamente los tres principios básicos de la seguridad de la información: la integridad, la confidencialidad y la disponibilidad de la información.

Este diagnóstico se realizará para conocer el estado actual de Seguridad y Privacidad de la Información utilizando las herramientas técnicas y metodológicas necesarias bajo el marco de referencia de Arquitectura TI. Lo anterior con el objetivo de poder contrarrestar los posibles ataques cibernéticos tanto internos como externos, minimizando al máximo el impacto ante la materialización de cualquier amenaza, situación de la que no está exenta ninguna institución. También permitirá mejorar los procesos y responder a los incidentes relacionados con la seguridad de la información de forma eficiente y efectiva.

5. MARCO DE REFERENCIA

5.1 MARCO TEÓRICO

El siguiente marco teórico que fundamenta este proyecto investigativo y de simulación permitirá tener a los lectores muchos conceptos y definiciones de forma clara y concisa que abarcan toda la terminología para determinar el nivel de seguridad y privacidad de la información del instituto

De acuerdo con el señor Antonio Villalón[1] existen muchas definiciones del término seguridad. Simplificando, y en general, podemos definir la seguridad como: "El conjunto de característica y normas aplicadas que indica que un sistema informático está libre de todo peligro, daño o riesgo."

Cuando se habla de seguridad de la información se está indicando que dicha información tiene una relevancia especial en un contexto determinado y que, por lo tanto, la información debe estar resguardada.

Desde las apariciones de los sistemas informáticos, la información se considera como un activo primordial y de mucho interés en las organizaciones debido a que con esa información se pueden tomar grandes decisiones que impactan el éxito o fracaso de la organización. Esta información inicialmente se guardaba en papel y se guardaba en grandes cantidades de abultados archivadores. Todos los datos de los usuarios o proveedores de la organización, o de los funcionarios quedaban registrados en papel, con todos los problemas que luego acarreaba su almacenaje, transporte, acceso y procesado.

Hoy en día gracias a los avances tecnológicos el proceso de la digitalización de la información de los grandes volúmenes de información se ha ido reduciendo cada día. Con este proceso sustancialmente se facilita y agiliza así la búsqueda, análisis

[1] VILLALON, Antonio. Seguridad En Unix Y Redes Versión 2.1 España. Julio, 2002. Disponible en http://gseguridad.unicauca.edu.co/articulos/unixsec.pdf.

y procesamiento de la información. Pero seguidamente con este proceso de digitalización surgen nuevos problemas asociados a la seguridad de la información, debido a que si es más fácil transportar la información también hay más probabilidades de que dicha información desaparezca 'en el camino'. Igualmente, si es más rápido acceder a ella también es más rápido modificar su contenido.
Desde la primera aparición de los grandes sistemas de información aislados y obsoletos hasta nuestros días, en los que el trabajo en red es lo más habitual, los problemas de la seguridad de la información han ido evolucionando en la medida que avanzan las nuevas tecnologías de la información.

Existen muchas definiciones sobre seguridad informática. La mayoría de los autores que hablan del tema se identifican con el concepto que ofrece la norma ISO/IEC 27001:1203 que dice:

La seguridad de la información está fundamentada en la conservación de tres términos los cuales se constituyen como los tres pilares sobre la que se cimienta todo el ente de la seguridad de la información: La confidencialidad, integridad y disponibilidad, así como también los sistemas implicados en su tratamiento, dentro de la organización.

• Confidencialidad: Es la propiedad mediante la cual se determina que la información solo se coloca a disposición de entidades, usuarios autorizados o procesos documentados y aprobados.

• Integridad: Se refiere al principio básico de conservar su originalidad, garantizado que la información sea confiable sin modificaciones no autorizadas.

• Disponibilidad: Este término se emplea para garantizar que la información o activos de información almacenada o trasmitida por cualquier medio siempre esté disponible solo al usuario o entidad autorizada.

La ISO/IEC 27001:2013, permite administrar la seguridad de la información de la mano con un proceso sistemático debidamente gestionado, documentado y fundamentado en el Modelo de privacidad seguridad de la información.[2]
Con esta norma se establecen varios mecanismos de control que permiten identificar y hacer frente para recuperarnos lo más rápido posible ante cualquier ataque cibernético o amenaza de seguridad, o evitar su materialización. También se establece el sistema de gestión de la continuidad del negocio, el cual va acompañado de auditorías internas y externas, las cuales le permiten identificar y verificar a qué riesgos están expuesto el instituto, si se emplean los controles establecidos para así minimizar el impacto ante las posibles incidentes de seguridad que se puedan presentar sobre el mismo, y poder garantizar la continuidad funcional del negocio.

El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo). Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente. Las medidas de seguridad (o controles) que se van a implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipos). Sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software, pero utilizan de una forma no segura; por lo tanto, la mayor parte de la implementación de ISO 27001 estará relacionada con determinar las reglas organizacionales (por ejemplo, redacción de documentos) necesarias para prevenir violaciones de la seguridad.

Como este tipo de implementación demandará la gestión de múltiples políticas, procedimientos, personas, bienes, etc., ISO 27001 ha detallado cómo amalgamar todos estos elementos dentro del sistema de gestión de seguridad de la información (SGSI). Por eso, la gestión de la seguridad de la información no se limita solamente a la seguridad de TI (por ejemplo, cortafuegos, anti-virus, etc.), sino que también

[2] ISO 27001.ES Sistema de Gestión de la Seguridad de la información, 2012. Disponible en http://www.iso27000.es

tiene que ver con la gestión de procesos, de los recursos humanos, con la protección jurídica y la protección física.

Para evitar incidentes es necesario contar con un plan de continuidad como respuesta prevista para aquellas situaciones de riesgo que se puedan afectar de forma crítica. En el pasado a este plan de continuidad se le conocía como plan de contingencias.

Según la estrategia de gobierno en línea La seguridad de la información de las organizaciones cobra cada vez mayor importancia, razón por la cual es más frecuente encontrar en ellas sistemas de gestión de la seguridad de la información, SGSI por lo tanto este diagnóstico es fundamental para el cumplimiento de las políticas y normas vigentes.

Para lograr un excelente diagnostico que identifique el nivel de seguridad de la información al interior del instituto se requiere soportar este proceso en normas como el conjunto de normas ISO 27000 de las cuales se destacan las ISO 27001, 27002 para los futuros pilares del SGSI. Es por esto que se toman como referencia para el desarrollo del proyecto, así como las metodologías de auditoría en los controles que en este caso cumplen con la misión de la organización que corresponde a la creación de aplicaciones web, para esto se necesario referenciar la metodología seleccionada en este caso COBIT, ya que abarcan la mayoría de las actividades de la institución.

5.1.1 Seguridad de la información modelo PDCA.

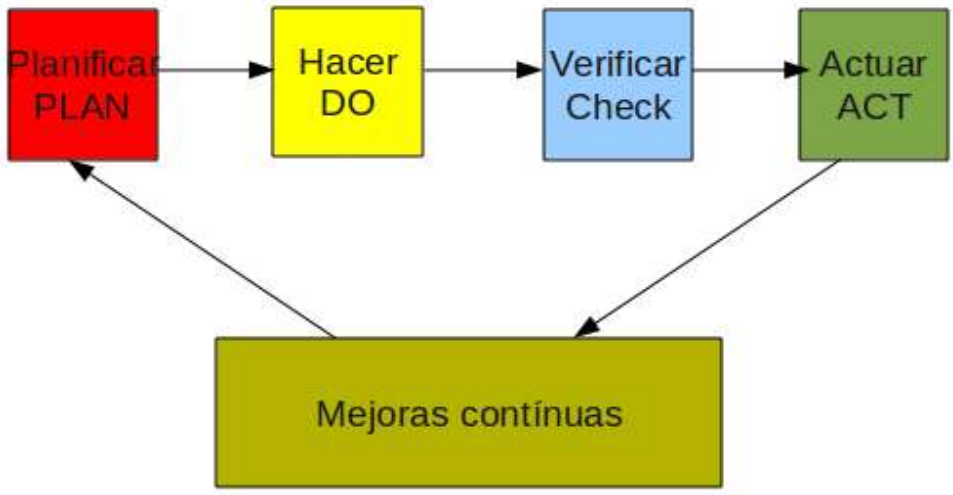
Dentro del Instituto el tema de la seguridad de la información es muy importante por lo tanto se requiere dedicarle tiempo y recursos. En el Instituto debe plantearse un Sistema de Gestión de la Seguridad de la Información (SGSI).

El objetivo de un SGSI es proteger la información y para ello lo primero que debe hacer un diagnóstico donde se identifiquen los 'activos de información' que deban ser protegidos y en qué grado.
Luego se debe aplicar el plan PDCA ('PLAN – DO – CHECK – ACT'), es decir Planificar, Hacer, Verificar, Actuar y volver a repetir el ciclo.

La seguridad de información no es producto final terminado que se pueda definir como un proceso que nunca termina ya que los riesgos nunca se eliminan, y están en constante evolución. Los riesgos no son solo de naturaleza tecnológica, y por lo tanto jamás se eliminan en su totalidad, sino que se mitigan.

Un SGSI por lo general cumple cuatro niveles redundantes:
Planificar, hacer, verificar y terminan en Actuar, consiguiendo así regenerar la seguridad.

Figura 1: Ciclo PHVA



Fuente:http://recursostic.educacion.es/observatorio/web/images/upload/elvira_mifsud/Introduccion_seguridad_html_m3824b9db.png

- PLANIFICAR (Plan): Es la etapa donde se analizan los tiempos, recursos, técnicas, metodología, normas políticas de seguridad, se determinan los controles junto con el análisis de aplicabilidad.

- HACER (Do): Aquí se realiza la implementación de los controles de cada dominio del MSPI en sintonía con el plan de riesgos.

- VERIFICAR (Check): Consiste en constatar con auditorias cada una de las actividades previamente descrita.

- ACTUAR (Act): Se refiere al proceso de poner en marcha las tareas de mantenimiento, actividades preventivas y correctivas, los planes de mejoramiento[3].

5.1.2 Modelo de seguridad y privacidad de la información.

MSPI es la sigla empleada para referirse al Modelo de Seguridad y Privacidad de la información, como un componente trasversal a la estrategia de gobierno en línea GEL, alineada a componente TIC. MSPI no es una cuestión solamente tecnológica o técnica de la oficina de tecnología de la información sino de la alta dirección, la cual tiene la responsabilidad de gestionar los riesgos y los impactos del negocio.

Desde el punto de vista del alcance del MSPI, desarrollado por el ministerio de las tecnologías de la información y las comunicaciones de Colombia (MINTIC), establece el conjunto de lineamientos, políticas, normas, procesos e instrucciones que provee y promueven la puesta en marcha, supervisión, mejora y control de la implementación del modelo, así como a la implementación de la Estrategia de gobierno en línea, establecida en manual GEL. El termino MSPI debe estar contemplado siempre en el Instituto.

A través del componente de TIC para Gobierno Abierto se alinea con el componente de Seguridad y Privacidad de la Información para buscar que la información de los usuarios internos y externos sea resguardada garantizando que la información se trate un tesoro valioso. También busca generar un plan de Seguridad y Privacidad de la Información alineado con el plan de negocio misional. Mejorando el nivel de confianza, mediante la identificación, determinación, mitigación de los riesgos de seguridad. Se puede decir que esta perspectiva de la estrategia de gobierno en línea esta afinada para el mejoramiento de los aspectos de la gestión pública, fomentando el dialogo realimentado entre las entidades públicas y los ciudadanos mediantes de acciones permanentes con el uso de canales electrónicos.

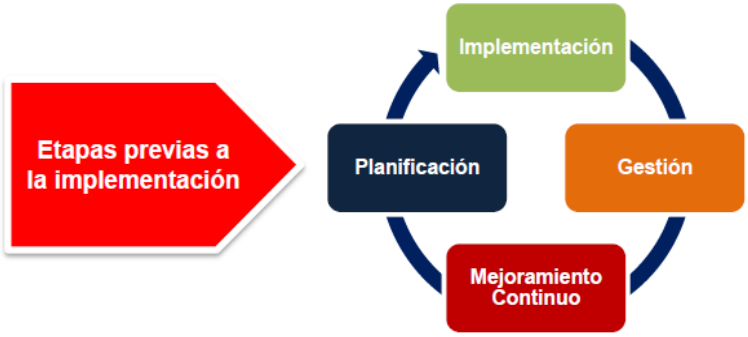
---

[3] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES Estrategia De Gobierno En Linea Articulo 8253 Modelo de Seguridad, 2016. Disponible en http://mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

5.1.3 Ciclo de operación del modelo de seguridad y privacidad de la información.

El modelo de seguridad y privacidad de la información está conformada por un ciclo de operación que consta de cinco (5) fases, las cuales hacen posible que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información de forma sostenible.

Figura 2: Gráfica del Modelo de Seguridad y Privacidad de la Información



Fuente: http://estrategia.gobiernoenlinea.gov.co/623/articles-8253_modelo_seguridad.pdf

La primera fase es el diagnóstico, en esta fase se enfocará la realización del proyecto por lo que se expresó en la formulación del problema que el instituto en la actualidad no cuenta con un diagnóstico al modelo de seguridad y privacidad de la información, donde se evalúen y se realice un control y seguimiento a los temas críticos de seguridad en las diferentes áreas.

5.1.4 Fase De Diagnóstico.

La fase de diagnóstico es fundamental ya que entrega los lineamientos para el trabajo a desarrollar en las fases siguientes. Desde el punto de vista de Seguridad de la Información, se enfatiza la capacidad de generar valor mediante el uso de políticas, estándares, procedimientos y buenas prácticas de seguridad que, en complemento con las TIC, conforman un sistema de gestión administrativo, sin embargo, el objetivo no es la incorporación de dichas tecnologías a la normativa

interna, sino la mejora de la gestión de los organismos a través de ellas. 4 Lo más importante en esta fase es identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

Figura 3: Etapa previas a la implantación

Fuente:http://estrategia.gobiernoenlinea.gov.co/623/articles-8253_modelo_seguridad.pdf

En la fase de diagnóstico del MSPI se pretende alcanzar las siguientes metas:[5]

Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior del instituto.

- Determinar el nivel de madurez de los controles de seguridad de la información.

[4] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES Estrategia De Gobierno En Linea Articulo 8253 Modelo de Seguridad, 2016. Disponible en http://mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf.
[5] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES Estrategia De Gobierno En Linea Articulo 8253 Modelo de Seguridad, 2016. Disponible en http://mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

- Identificar el avance de la implementación del ciclo de operación al interior del instituto.

- Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.

- Identificación del uso de buenas prácticas en ciberseguridad.

Para realizar dicha fase las entidades deben efectuar la recolección de la información con la ayuda de la herramienta de diagnóstico y la metodología de pruebas de efectividad.

Una vez se tenga el resultado del diagnóstico inicial y se haya determinado el nivel de madurez del instituto se procede al desarrollo de la fase de Planificación. Los resultados asociados a la fase de Diagnostico previas a la implementación deben ser revisados y socializados por las partes interesadas.

Se podría resumir de gran manera que la seguridad de la información está conformada por un conjunto de medidas técnicas, organizativas y legales que permiten a las organizaciones garantizar los tres pilares fundamentales de la información, como lo son: la confidencialidad, integridad y disponibilidad de cualquier sistema de información.

5.2 MARCO CONCEPTUAL

Identificación de activos de información: de acuerdo con la norma ISO/IE 27001, “activo de información” se define como cualquier elemento que tenga valor para la organización y, en consecuencia, deba ser protegido.

La clasificación de activos de información se debe realizar acorde con el alcance definido para la implementación del MSPI (es decir a los procesos en los que se implementara seguridad de la información) la gestión de activos debe estar alineada con el Dominio 8 Gestión de Activos del anexo A de la norma ISO 27001:2013, y la

guía de controles del modelo de seguridad y privacidad de la información, para garantizar el cumplimiento de los puntos descritos a continuación:[6]

Inventario de activos: se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.

Propiedad de los activos: los activos mantenidos en el inventario corresponderían a cada uno de los propietarios.

Uso aceptable de los activos: se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.

Devolución de activos: todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.

Clasificación de la información: la información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.

Etiquetado de la información: se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.

[6] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES Estrategia De Gobierno Guia 5 para la gestión y clasificación de activos de información 2016. Disponible en http://mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_clasificacion.pdf

Manejo de activos: se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.

Información: conjunto de datos procesados y relacionados que tienen significado para la toma de decisiones en el instituto. La información es un activo que, como otros activos importantes de la organización, es esencial para las actividades del instituto y, en consecuencia, necesita una protección adecuada.

La definición dada por la ley 1712 del 2014, se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.

Información pública: es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad.

Información pública clasificada: es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semi-privado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 del 2014.

Información pública reservada: es la información que estando en poder de un sujeto, es exceptuada, de acceso a la ciudadanía por daño a intereses públicos y bajo el cumplimiento de la totalidad de los requisitos consagrados en el artículo de esta ley.

Clasificación de la Información: es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en el instituto. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado.

Propietario de la Información: es una parte designada del instituto, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar.

Periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso.

Custodio: es una parte designada del instituto, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado.

Usuario: Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la Unidad, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información.

Vulnerabilidad: en el campo de la informática, la vulnerabilidad es el punto o aspecto del sistema que es susceptible de ser atacado o de dañar la seguridad del mismo. Representan las debilidades o aspectos falibles o atacables en el sistema informático.[7]

5.2.1 Tipos de amenazas informáticas.

Hay diversas clasificaciones de las amenazas al sistema informático, todo depende del punto de vista cómo se analicen. Una primera clasificación es según el efecto causado en el sistema, las amenazas pueden clasificarse en cuatro tipos:

- Intercepción
- Modificación
- Interrupción
- Generación

[7]MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES Estrategia De Gobierno Guia 5 para la gestión y clasificación de activos de información 2016. Disponible en http://mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_clasificacion.pdf.

Intercepción: cuando una persona, programa o proceso logra el acceso a una parte del sistema a la que no está autorizada. Por ejemplo, la escucha de una línea de datos, o las copias de programas o archivos de datos no autorizados. Estas son más difíciles de detectar ya que en la mayoría de los casos no alteran la información o el sistema.

Modificación: este tipo de amenaza se trata no sólo de acceder a una parte del sistema a la que no se tiene autorización, sino también de cambiar su contenido o modo de funcionamiento. Por ejemplo, el cambiar el contenido de una base de datos, o cambiar líneas de código en un programa.

Interrupción: se trata de la interrupción mediante el uso de algún método el funcionamiento del sistema. Por ejemplo, la saturación de la memoria o máximo de procesos en el sistema operativo, la destrucción de algún dispositivo hardware.

Generación: generalmente se refiere a la posibilidad de añadir información a programas no autorizados en el sistema. Por ejemplo, el añadir campos y registros en una base de datos, o adicionar código en un programa (virus).

Análisis de Riesgos: es una herramienta de diagnóstico que permite establecer la exposición real a los riesgos por parte de una organización. Este análisis tiene como los siguientes objetivos la identificación de los riesgos (mediante la identificación de sus elementos), lograr establecer el riesgo total y posteriormente el riesgo residual luego de aplicadas las contramedidas en términos cuantitativos o cualitativos.

Estándar Cobit empleada para el Análisis y Evaluación de Riesgos de TI: Modelo para evaluar y/o auditar la gestión y control de los de Sistemas de Información y Tecnología relacionada (IT).

SGSI: Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, Información es el conjunto de datos organizados en poder de una entidad que posean valor para la misma, indistintamente como se guarde o transmita (escrita, imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en

conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.[8]

5.3 MARCO LEGAL

La seguridad informática, es la especialidad del área de la informática, que se concentra en la protección de los activos de infraestructura física y lógica computacional y todo lo relacionado con esta. Por lo tanto existen una serie de normas, leyes, reglas, herramientas legislativas que rigen todo el tema de la seguridad de la información.

En el año 2009 el congreso de la República Colombiana promulgó la Ley 1273, con la cual se actualiza el Código Penal, creando un nuevo bien jurídico protector denominado “De la Protección de la información y de los datos” esta ley regula los delitos informáticos preservando integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.[9]

Esta ley consta de los siguientes artículos, los cuales se citan literalmente: Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en

---

[8] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES Estrategia De Gobierno En Linea Articulo 8253 Modelo de Seguridad, 2016. Disponible en http://mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf.
[9] DELTAASESORES.COM Delitos Informáticos en Colombia, 2014 Disponible en

pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269E: USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

La información es el activo más importante en el mundo actual, es por ello que el 17 de octubre de 2012 el Gobierno Nacional expidió la Ley Estatutaria 1581 de 2012 mediante la cual se dictan disposiciones generales para la protección de datos personales, en ella se regula el derecho fundamental de hábeas data y se señala la importancia en el tratamiento del mismo tal como lo corrobora la Sentencia de la Corte Constitucional C – 748 de 2011 donde se estableció el control de constitucionalidad de la Ley en mención. La nueva ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como la recolección, almacenamiento, uso, circulación o

supresión (en adelante tratamiento) por parte de entidades de naturaleza pública y privada.[10], esta ley consta de algunos artículos como son:

Artículo 4°. Principios para el Tratamiento de datos personales**.** En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios:

a) Principio de legalidad en materia de Tratamiento de datos: El Tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen.

b) Principio de finalidad**:** El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.

c) Principio de libertad: El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

d) Principio de veracidad o calidad: La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

e) Principio de transparencia: En el Tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

[10] COLOMBIADIGITAL.NET ABC para proteger los datos personales ley 1581 decreto 1377 2012.

f) Principio de acceso y circulación restringida: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley.

Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley.

g) Principio de seguridad: La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

h) Principio de confidencialidad: Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma. [11]

[11] ALCALDIADEBOGOTA.GOV.CO normas 49981 2013.

6. METODOLOGÍA

Parra llevar a cabo el presente proyecto se desarrolló la siguiente metodología:

Figura 4: Metodología general

Fuente: el autor

Estas fases y modelos han sido establecidos para ofrecer una guía para el establecimiento, implementación, operación, seguimiento, revisión y mejora de un Sistema de Gestión de la Seguridad de la Información (SGSI). La adopción de este sistema es una decisión de tipo estratégico. El diseño y la posterior implementación del SGSI, deben estar basados en el tamaño, la estructura, las necesidades, los objetivos y los procesos del IMN.

A continuación haremos una descripción detallada de las cuatro (4) fases que se realizaron:

FASE 1. LEVANTAMIENTO DE INFORMACION: Para el levantamiento de la información se elaborarán cuestionarios, entrevistas e Inspecciones en sitio, consolidación de resultados, análisis de resultados, elaboración de informes y plan de acción.

En esta fase se presentará el Informe ejecutivo del análisis de GAP realizado en el Instituto con respecto a la NTC/ISO 27001:2013 con el fin de comprender el estado general de madurez de la seguridad de la información dentro del instituto.

FASE 2. IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS: En esta fase se definirá el procedimiento de identificación, valoración y clasificación de los activos de información del Instituto mediante algunas entrevistas.

FASE 3. GESTIÓN DEL RIESGO: Durante esta fase se realizarán entrevistas con el fin de comprender qué riesgos pueden afectar la confidencialidad, la integridad y la disponibilidad de la información del instituto. También se revisaron la información de los procesos: categorización, procedimientos y mapas de riesgo. Finalmente, para entender el contexto de la organización se deben entender los factores tanto internos como externos que pueden llegar a afectar la información propiedad del IMN.

FASE 4. PRUEBAS DE VULNERABILIDADES: En esta fase se realizan las pruebas de penetración, análisis de vulnerabilidades con el fin de comprobar o medir el nivel de eficiencia de la implementación del MSPI y demás actividades con sus respectivas remediaciones de los equipos informáticos propuestos por el IMN.

7. DESARROLLO DEL PROYECTO

DIAGNÓSTICO BASADO EN LA NORMA ISO 27001:2013

8. FASE 1. LEVANTAMIENTO DE LA INFORMACIÓN

Esta primera fase es de mucha importancia y dedicación, ya que se constituye en la materia prima e insumo para las siguientes fases con el cumplimento de los objetivos en que se enfocó la realización del proyecto, como se expresó en el planteamiento del problema que el instituto en la actualidad no cuenta con un diagnóstico al modelo de seguridad y privacidad de la información, donde se evalúen y se realice un control y seguimiento a los temas críticos de seguridad en las diferentes áreas.

La seguridad de la información es un componente crítico dentro de la estrategia de Gobierno en Línea y recomienda realizar un análisis de brecha para conocer el estado de madurez de la seguridad de la información antes de iniciar el establecimiento de un Sistema de Gestión de la Seguridad de la Información (SGSI).

El Análisis Gap realizado en el instituto contempló tres (3) procesos de apoyo: Gestión de información y tecnologías, gestión integral del talento humano y gestión de adquisición de bienes y servicios.

El diagnóstico se basa teniendo en cuenta los dominios del anexo A de la norma NTC/ISO 27001:2013 (Ver Tabla No. 1) y el Modelo de Seguridad y Privacidad de la Información V.3.0.2 – MPSI de la Estrategia de Gobierno en Línea - GEL.

Tabla 1: Dominios de la norma

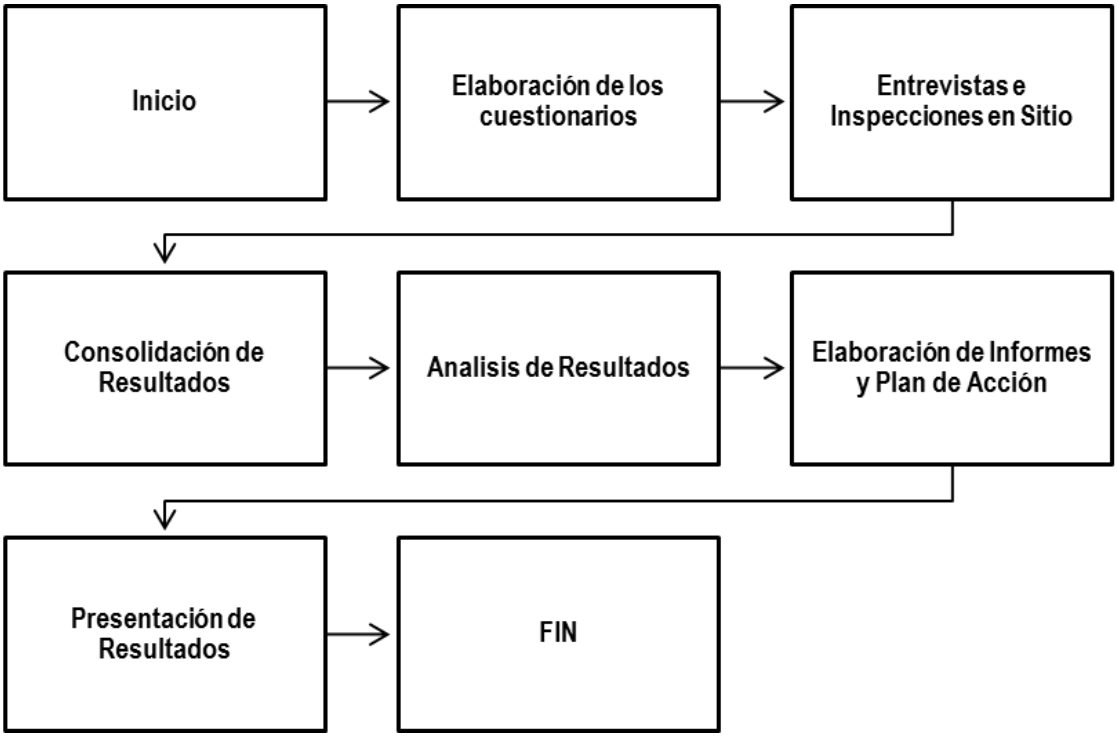
Dominio ISO 27001	Objetivo de control
Política de seguridad.	Objetivo de control A.5
Organización de la seguridad de la información.	Objetivo de control A.6
Seguridad de los RRHH.	Objetivo de control A.7
Gestión de activos.	Objetivo de control A.8
Control de accesos.	Objetivo de control A.9
Criptografía.	Objetivo de control A.10
Seguridad física y ambiental.	Objetivo de control A.11
Seguridad en las operaciones.	Objetivo de control A.12
Seguridad en las comunicaciones.	Objetivo de control A.13
Adquisición de sistemas, desarrollo y mantenimiento.	Objetivo de control A.14
Relación con proveedores.	Objetivo de control A.15
Gestión de los incidentes de seguridad.	Objetivo de control A.16
Continuidad del negocio.	Objetivo de control A.17
Cumplimiento con requerimientos legales y contractuales.	Objetivo de control A.18

Fuente: El autor

El proceso llevado a cabo para el determinar el diagnóstico del estado de madurez se representa fue el siguiente:

Los pasos que se realizaron para llegar a este análisis GAP (análisis de brecha) con relación a la NTC/ISO 27001:2013 y el MSPI. El GAP en donde se tuvo en cuenta los diferentes dominios de la NTC/ISO 27001:2013 fue:

Figura 5: Pasos del análisis GAP



Fuente: El autor

PASO 1. Elaboración de los cuestionarios. En esta fase se realizaron las siguientes actividades:

1. Revisión de la NTC/ISO 27001:2013 y del MSPI
2. Elaboración de un conjunto de preguntas por cláusula y dominio
3. Definición de niveles y criterios de madurez
4. Implementación de la herramienta

A continuación, se presentan los niveles y criterios teniendo en cuenta el MSPI[12]:

Tabla 2: Niveles y criterios de madurez

NIVEL	PORCENTAJE	CRITERIOS
Inexistente	0%	No se cuenta con la cláusula o control. No se reconoce la información como un activo importante para el logro de la misión y visión del instituto.
Inicial	1-20%	El control esta implementado no obstante el modelo de seguridad de políticas, procedimientos y estándares de configuración, no existe.
Repetible	21-40%	El control esta implementado y además es soportado por un documento que contiene una política de alto nivel y otras políticas operativas debidamente aprobadas.
Definido	41-60%	El control esta implementado y soportado por políticas, procedimientos y estándares de configuración debidamente publicados y socializados.
Administrado	61-80%	En este nivel se realizan mediciones sobre la efectividad de los controles.
Optimizado	81-100%	En este nivel se encuentran las entidades en las cuales se mide la efectividad de los controles con el fin de mejorarlos y optimizarlos.

Fuente: Estrategia de Gobierno en Línea - GEL

[12] Modelo de Seguridad y Privacidad de la Información V.3.0.2 – MPSI de la Estrategia de Gobierno en Línea - GEL

PASO 2. Entrevistas e inspecciones en sitio.

En esta fase se realizaron las siguientes actividades:

1. Entendimiento de la estructura organizacional
2. Revisión de los perfiles, cargos y caracterización de los procesos
3. Elaboración agenda preliminar
4. Revisión y aprobación de la agenda preliminar
5. Ejecución de las entrevistas e inspecciones en sitio

PASO 3. Consolidación de resultados:

En esta fase se realizaron las siguientes actividades:

1. Calificación del nivel de madurez de las cláusulas
2. Calificación del nivel de madurez de los dominios
3. Revisión de calificaciones
4. Revisión de observaciones y hallazgos

PASO 4. Análisis de resultados:

En esta fase se realizaron las siguientes actividades:

1. Calculo del promedio por cada cláusula
2. Calculo del promedio por cada dominio
3. Calculo del promedio por cada control
4. Elaboración de graficas de madurez y brecha
5. Selección de hallazgos más críticos

PASO 5. Elaboración de informes y plan de acción

En esta fase se realizaron las siguientes actividades:

1. Definición de objetivos, alcance y marco teórico
2. Presentación de principales hallazgos
3. Elaboración de recomendaciones
4. Definición de dominios críticos

5. Definición de controles críticos
6. Definición de los plazos de implementación

PASO 6. Presentación de resultados:

En esta fase se realizarán las siguientes actividades:

1. Selección de los puntos más relevantes del informe
2. Elaboración de presentación ejecutiva
3. Revisión por parte del instituto, de la presentación ejecutiva
4. Ajustes a la presentación
5. Convocatoria
6. Presentación

8.1 INFORME DE RESULTADOS DEL DIAGNOSTICO DE SEGURIDAD DE LA INFORMACIÓN

8.1.1 Política de seguridad de la información.

A continuación se presenta los resultados obtenidos para el Dominio A.5 Políticas de Seguridad de la Información en donde se muestra el promedio por control, dominio, y los principales hallazgos y recomendaciones:

Tabla 3: Política de seguridad de la información

A.5	POLÍTICA DE SEGURIDAD	PROMEDIO POR DOMINIO	30 %	PRINCIPALES HALLAZGOS Y RECOMENDACIONES
A.5.1	Directrices establecidas por la Dirección para la Seguridad de la Información	Promedio por control	30 %	Se pudo evidenciar que existe un documento de Políticas de seguridad de la información (GT-PI-POL-001), el cual se encuentra aprobado y publicado en el aplicativo que administra los documentos, no obstante, las políticas están alineadas a la versión 2005 de la NTC/ISO 27001 y no han sido formalmente socializadas. Así mismo, se recomienda que las política sean revisadas al menos una vez al año o cuando ocurra un cambio significativo en el instituto o su entorno.
A.5.1.1	Políticas para la seguridad de la información	% por Control	60 %	
A.5.1.2	Revisión de la política de seguridad de la información	% por Control	0%	

Fuente: El autor

8.1.2 Organización de la Seguridad de la Información.

A continuación se presenta los resultados obtenidos para el Dominio A.6 Organización de la Seguridad de la Información en donde se muestra el promedio por control, dominio, y los principales hallazgos y recomendaciones:

Tabla 4: Organización de la seguridad de la información

A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	PROMEDIO POR DOMINIO	13%	PRINCIPALES HALLAZGOS Y RECOMENDACIONES
A.6.1	Organización Interna	Promedio por control	17%	Actualmente, los roles y responsabilidades de seguridad de la información están en cabeza de la Oficina de Tecnologías de la Información, no obstante, es recomendable que esta oficina tenga el apoyo, la colaboración y la suficiencia de recursos desde la alta dirección. Es importante también, que exista una política sobre el uso de Dispositivos Móviles con el fin de evitar posibles riesgos de seguridad de la información que puedan impactar la reputación del instituto.
A.6.1.1	Asignación de responsabilidades para la seguridad de la información	% por Control	0%	
A.6.1.2	Separación de tareas	% por Control	0%	
A.6.1.3	Contacto con las autoridades	% por Control	40%	
A.6.1.4	Contacto con grupos de interés especiales	% por Control	60%	
A.6.1.5	Seguridad de la información en la gestión de proyectos	% por Control	0%	
A.6.2	Dispositivos móviles	Promedio por control	10%	
A.6.2.1	Computación móvil y trabajo remoto	% por Control	0%	
A.6.2.2	Trabajo remoto	% por Control	20%	

Fuente: El autor

8.1.3 Seguridad de los recursos humanos.

A continuación se presenta los resultados obtenidos para el Dominio A.7 Seguridad de los Recursos Humanos en donde se muestra el promedio por control, dominio, y los principales hallazgos y recomendaciones:

Tabla 5: Seguridad de los recursos humanos

A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	PROMEDIO POR DOMINIO	73%	PRINCIPALES HALLAZGOS Y RECOMENDACIONES
A.7.1	Antes de asumir el empleo	Promedio por control	100%	Durante las entrevistas, se evidenció que la vinculación de los funcionarios al instituto se hace acatando la Ley 909 de 2004, lo que garantiza que se realice una selección de personal segura. Por otra parte, es recomendable contar con programas de educación,
A.7.1.1	Selección	% por Control	100%	
A.7.1.2	Términos y condiciones laborales	% por Control	100%	
A.7.2	Durante la vigencia del contrato laboral	Promedio Control	80%	

A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	PROMEDIO POR DOMINIO	73%	PRINCIPALES HALLAZGOS Y RECOMENDACIONES
A.7.2.1	Responsabilidades de la dirección	% por Control	100%	entrenamiento y sensibilización en seguridad de la información debidamente formalizados. El Talento humano es uno de los componentes más importantes que debe considerarse para lograr la efectividad del SGSI, sin su compromiso y adecuada cultura se dificulta el logro de los objetivos de seguridad de la información.
A.7.2.2	Educación, formación y sensibilización en seguridad de la información	% por Control	40%	
A.7.2.3	Proceso disciplinario	% por Control	100%	
A.7.3	Terminación o cambio de la contratación laboral	Promedio por control	40%	
A.7.3.1	Responsabilidades en la terminación	% por Control	40%	

Fuente: El autor

8.1.4 Gestión de activos.

A continuación se presenta los resultados obtenidos para el Dominio A.8 Gestión de Activos en donde se muestra el promedio por control, dominio, y los principales hallazgos y recomendaciones:

Tabla 6: Gestión de activos

A.8	GESTION DE ACTIVOS	PROMEDIO POR DOMINIO	13%	PRINCIPALES HALLAZGOS Y RECOMENDACIONES
A.8.1	Responsabilidad por los activos	Promedio por control	0%	Se evidenció durante las entrevistas que el instituto cuenta con un inventario de bienes e inmuebles bastante maduro, aunque éste no contempla activos de seguridad de la información, lo que conlleva a la ausencia de un sistema de clasificación y etiquetado de la información. Se recomienda contar con política y procedimientos para el borrado y destrucción de los medios.
A.8.1.1	Inventario de activos	% por Control	0%	
A.8.1.2	Propiedad de los activos	% por Control	0%	
A.8.1.3	Uso aceptable de los activos	% por Control	0%	
A.8.1.4	Devolución de los activos	% por Control	0%	
A.8.2	Clasificación de la información	Promedio por control	13%	
A.8.2.1	Clasificación de la información	% por Control	20%	
A.8.2.2	Etiquetado de la información	% por Control	0%	
A.8.2.3	Manejo de activos	% por Control	20%	
A.8.3	Manejo de medios	Promedio por control	27%	
A.8.3.2	Disposición de los medios	% por Control	20%	
A.8.3.3	Transferencia de medios físicos	% por Control	20%	

Fuente: El autor

8.1.5 Control de acceso.

A continuación se presenta los resultados obtenidos para el Dominio A.9 Control de Acceso en donde se muestra el promedio por control, dominio, y los principales hallazgos y recomendaciones:

Tabla 7: Control de Acceso

A.9	CONTROL DE ACCESO	PROMEDIO POR DOMINIO	34%	PRINCIPALES HALLAZGOS Y RECOMENDACIONES
A.9.1	Requisitos del negocio para control de acceso	Promedio por control	30%	Se cuenta con una Política de Control de acceso lógico aunque ésta no está debidamente socializada, también se pudo constatar que existe un controlador de dominio el cual realiza las funciones de autenticación, autorización y gestión de registros junto con la gestión de contraseñas. A nivel de redes se cuenta con un esquema de segmentación utilizando redes virtuales. Se recomienda contar con procedimientos para que los usuarios que se desvinculan del instituto sean debidamente eliminados del sistema.
A.9.1.1	Política de control de acceso	% por Control	20%	
A.9.1.2	Acceso a redes y servicios de red	% por Control	40%	
A.9.2	Gestión de acceso a usuarios	Promedio por control	30%	
A.9.2.1	Registro y cancelación de usuarios	% por Control	40%	
A.9.2.2	Suministro de acceso de usuarios	% por Control	60%	
A.9.2.3	Gestión de derechos de acceso privilegiado	% por Control	0%	
A.9.2.4	Gestión de información secreta para la autenticación de usuarios	% por Control	60%	
A.9.2.5	Revisión de los derechos de acceso de usuarios	% por Control	0%	
A.9.2.6	Retiro o ajuste de los derechos de acceso	% por Control	20%	
A.9.3	Responsabilidades de los usuarios	Promedio por control	40%	
A.9.3.1	Uso de información secreta para la autenticación	% por Control	40%	
A.9.4	Control de acceso a sistemas y aplicaciones	Promedio por control	36%	
A.9.4.1	Restricción de acceso a la información	% por Control	40%	
A.9.4.2	Procedimiento de ingreso seguro	% por Control	40%	
A.9.4.3	Sistema de gestión de contraseñas	% por Control	40%	
A.9.4.4	Uso de programas utilitarios privilegiados	% por Control	0%	
A.9.4.5	Control de acceso a códigos fuente de programas	% por Control	60%	

Fuente: El autor

8.1.6 Criptografía.

A continuación se presenta los resultados obtenidos para el Dominio A.10 Criptografía en donde se muestra el promedio por control, dominio, y los principales hallazgos y recomendaciones:

Tabla 8: Criptografía

A.10	CRIPTOGRAFÍA	PROMEDIO POR DOMINIO	20%	PRINCIPALES HALLAZGOS Y RECOMENDACIONES
A.10.1	Controles criptográficos	Promedio por control	20%	Se recomienda contar por lo menos con una política de uso de controles criptográficos, la cual sea aplicada siguiendo las normas vigentes nacionales, teniendo en cuenta los niveles de confidencialidad de la información y que los algoritmos utilizados sean seguros.
A.10.1.1	Política de uso de controles criptográficos	% por Control	0%	
A.10.1.2	Gestión de llaves	% por Control	40%	

Fuente: El autor

8.1.7 Seguridad física.

A continuación se presenta los resultados obtenidos para el Dominio A.11 Seguridad Física en donde se muestra el promedio por control, dominio, y los principales hallazgos y recomendaciones:

Tabla 9: Seguridad física

A.11	SEGURIDAD FÍSICA	PROMEDIO POR DOMINIO	38%	PRINCIPALES HALLAZGOS Y RECOMENDACIONES
A.11.1	Áreas seguras	Promedio por control	43%	Tanto la seguridad física como la seguridad lógica, deben ser una prioridad dentro de los esfuerzos tendientes a garantizar la seguridad de la información. La ubicación del DATACENTER, el material de construcción de su perímetro, la organización del cableado, las condiciones de limpieza, los sistemas de monitorización, la presencia de material combustible y el aseguramiento de los racks, son elementos que representan riesgos a la seguridad de la información.
A.11.1.1	Perímetro de seguridad física	% por control	60%	
A.11.1.2	Controles de acceso físico	% por control	60%	
A.11.1.3	Seguridad en oficinas, recintos e instalaciones	% por control	20%	
A.11.1.4	Protección contra amenazas externas y ambientales	% por control	60%	
A.11.1.5	Trabajo en áreas seguras	% por control	60%	
A.11.1.6	Áreas de carga, despacho y acceso público	% por control	0%	
A.11.2	Seguridad de los equipos	Promedio por control	33%	
A.11.2.1	Ubicación y protección de los equipos	% por control	20%	
A.11.2.2	Servicios de suministro	% por control	60%	
A.11.2.3	Seguridad del cableado	% por control	60%	

A.11	SEGURIDAD FÍSICA	PROMEDIO POR DOMINIO	38%	PRINCIPALES HALLAZGOS Y RECOMENDACIONES
A.11.2.4	Mantenimiento de los equipos	% por control	40%	
A.11.2.5	Salida de equipos	% por control	60%	
A.11.2.6	Seguridad de los equipos fuera de las instalaciones	% por control	0%	
A.11.2.7	Seguridad en la reutilización o eliminación de los equipos	% por control	0%	
A.11.2.8	Equipos no atendidos	% por control	40%	
A.11.2.9	Política de escritorio y pantallas limpias	% por control	20%	

Fuente: El autor

8.1.8 Gestión de operaciones.

Dominio A.12 Gestión de Operaciones en donde se muestra el promedio por control, dominio, y los principales hallazgos y recomendaciones:

Tabla 10: Gestión de operaciones

A.12	GESTIÓN DE OPERACIONES	PROMEDIO POR DOMINIO	23%	PRINCIPALES HALLAZGOS Y RECOMENDACIONES
A.12.1	Procedimientos operacionales y responsabilidades	Promedio por control	28%	Las políticas y los procedimientos son parte fundamental de un modelo de seguridad. Los procedimientos permiten realizar ciertas actividades de manera segura, estos deben estar revisados, aprobados, publicados, comunicados y socializados, para asegurar su adecuada utilización. Por otra parte, la gestión de cambios debe estar soportada por políticas y procedimientos, y debe contemplar los riesgos asociados al cambio. Así mismo, el registro de todos los eventos es importante para la gestión de los incidentes de seguridad. Finalmente a todos los sistemas se les debe realizar un análisis de vulnerabilidad al menos una vez al año acompañado de un plan de remediación.
A.12.1.1	Documentación de los procedimientos de operación	% por control	40%	
A.12.1.2	Gestión del cambio	% por control	0%	
A.12.1.3	Gestión de la capacidad	% por control	0%	
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	% por control	60%	
A.12.1.5	Protección contra código malicioso	% por control	40%	
A.12.2	Respaldo	Promedio por control	60%	
A.12.2.1	Respaldo de la información	% por control	60%	
A.12.3	Registro y seguimiento	Promedio por control	20%	
A.12.3.1	Registro de eventos	% por control	20%	
A.12.3.2	Protección de la información de registro	% por control	0%	
A.12.3.3	Registros del administrador y del operador	% por control	20%	
A.12.3.4	Sincronización de relojes	% por control	40%	
A.12.4	Control del software en operación	Promedio por control	0%	
A.12.4.1	Instalación del software en sistemas en operación	% por control	0%	
A.12.5	Gestión de la vulnerabilidad técnica	Promedio por control	30%	
A.12.5.1	Gestión de las vulnerabilidades técnicas	% por control	40%	
A.12.5.2	Restricciones en la instalación de software	% por control	20%	
A.12.6	Consideraciones de auditoría para los sistemas de información	Promedio por control	0%	
A.12.6.1	Controles de auditoría sobre los sistemas de información	% por control	0%	

Fuente: El autor

8.1.9 Seguridad de las comunicaciones.

A continuación se presenta los resultados obtenidos para el Dominio A.13 Seguridad de las Comunicaciones en donde se muestra el promedio por control, dominio, y los principales hallazgos y recomendaciones:

Tabla 11: Seguridad de las comunicaciones

A.13	SEGURIDAD DE LAS COMUNICACIONES	PROMEDIO POR DOMINIO	20%	PRINCIPALES HALLAZGOS Y RECOMENDACIONES
A.13.1	**Gestión de la Seguridad de las Redes**	**Promedio por control**	40%	Se deben tener políticas y procedimientos para la transferencia de información a otras entidades. Los elementos de red deben enviar sus registros a un servidor centralizado y deben existir estándares de configuración seguros.
A.13.1.1	**Control de redes**	**% por control**	40%	
A.13.1.2	**Seguridad de los servicios de red**	**% por control**	60%	
A.13.1.3	**Separación en las redes**	**% por control**	20%	
A.13.2	**Transferencia de Información**	**Promedio por control**	0%	
A.13.2.1	**Políticas y Procedimientos de transferencia de Información**	**% por control**	0%	
A.13.2.2	**Acuerdos sobre transferencia de Información**	**% por control**	0%	
A.13.2.3	**Mensajería Electrónica**	**% por control**	0%	
A.13.2.4	**Acuerdos de Confidencialidad o de no divulgación**	**% por control**	0%	

Fuente: El autor

8.1.10 Adquisición, desarrollo y mantenimiento de sistemas.

A continuación se presenta los resultados obtenidos para el Dominio A.14 Adquisición, Desarrollo y Mantenimiento de Sistemas en donde se muestra el promedio por control, dominio, y los principales hallazgos y recomendaciones:

Tabla 12: Adquisición, desarrollo y mantenimiento de sistemas

A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	PROMEDIO POR DOMINIO	19%	PRINCIPALES HALLAZGOS Y RECOMENDACIONES
A.14.1	Requisitos de seguridad de los sistemas de información	Promedio por control	27%	La seguridad de la información debe ser considerada en todo el ciclo de desarrollo (SDLC). Es recomendable contar con políticas y procedimientos para el desarrollo seguro, junto con herramientas de software que permitan la identificación de líneas de código inseguro. Finalmente el entrenamiento, la educación y la sensibilización en seguridad de la información deben ser impartidos de manera formal a todos los desarrolladores.
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	% por control	0%	
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	% por control	80%	
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	% por control	0%	
A.14.2	Seguridad en los procesos de desarrollo y soporte de software	Promedio por control	29%	
A.14.2.1	Política de desarrollo de software	% por control	20%	
A.14.2.2	Procedimiento de control de cambios de sistemas	% por control	20%	
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	% por control	40%	
A.14.2.4	Restricciones en los cambios a los paquetes de software	% por control	40%	
A.14.2.5	Principios de construcción de sistemas seguros	% por control	0%	
A.14.2.6	Ambientes de desarrollo seguro	% por control	40%	
A.14.2.7	Desarrollo contratado externamente	% por control	0%	
A.14.2.8	Pruebas de seguridad de los sistemas	% por control	0%	
A.14.2.9	Pruebas de aceptación de los sistemas	% por control	100 %	
A.14.3	Datos de prueba	Promedio por control	0%	
A.14.3.1	Protección de datos de prueba	% por control	0%	

Fuente: El autor

8.1.11 Relaciones Con Los Proveedores.

A continuación se presenta los resultados obtenidos para el Dominio A.15 Relaciones con los Proveedores en donde se muestra el promedio por control, dominio, y los principales hallazgos y recomendaciones:

Tabla 13: Relaciones con los proveedores

A.15	RELACIONES CON LOS PROVEEDORES	PROMEDIO POR DOMINIO	15%	PRINCIPALES HALLAZGOS Y RECOMENDACIONES
A.15.1	Seguridad de la información en el manejo de proveedores	Promedio por control	10%	Se debe contar con una política, procedimientos, formatos y guías para gestionar la relación con los proveedores en cuanto a la seguridad de la información. Los contratos con los proveedores deben establecer cláusulas para el cuidado de la información. La ejecución de estos contratos debe ser supervisada para garantizar la confidencialidad, disponibilidad e integridad y todo cambio al contrato debe considerar los riesgos asociados a la información.
A.15.1.1	Política de seguridad en el manejo con los proveedores	% de control	20%	
A.15.1.2	Tratamiento de la seguridad de la información dentro del acuerdo con proveedores	% de control	20%	
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	% de control	0%	
A.15.2	Gestión de la prestación de servicios de proveedores	Promedio por control	20%	
A.15.2.1	Seguimiento y revisión de los servicios con los proveedores	% de control	40%	
A.15.2.2	Gestión de los cambios en los servicios de terceras partes	% de control	0%	

Fuente: El autor

8.1.12 Gestión de incidentes de seguridad de la información.

A continuación se presenta los resultados obtenidos para el Dominio A.16 Gestión de Incidentes de Seguridad de la Información en donde se muestra el promedio por control, dominio, y los principales hallazgos y recomendaciones:

Tabla 14: Gestión de incidentes de seguridad de la información

A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD	PROMEDIO POR DOMINIO	14%	PRINCIPALES HALLAZGOS Y RECOMENDACIONES
A.16.1	Gestión de Incidentes y mejoras en la seguridad de la información	Promedio por control	14%	Para lograr una gestión consistente y efectiva de los incidentes de seguridad de la información se deben establecer: por un lado, asignación de responsabilidades y por el otro, procedimientos detallados para clasificar, dar respuesta, escalamiento, solución, aprendizaje y registro de estos incidentes. Se recomienda realizar un programa de socialización a
A.16.1.1	Responsabilidades y procedimientos	% por control	40%	
A.16.1.2	Reporte de eventos de seguridad de la información	% por control	20%	
A.16.1.3	Reporte de debilidades de seguridad de la información	% por control	20%	
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	% por control	20%	
A.16.1.5	Respuesta a incidentes de seguridad de la información	% por control	0%	

A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD	PROMEDIO POR DOMINIO	14%	PRINCIPALES HALLAZGOS Y RECOMENDACIONES
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	% por control	0%	funcionarios, contratistas y proveedores, para que reporten eventos de seguridad a la mayor brevedad posible.
A.16.1.7	Recolección de evidencia	% por control	0%	

Fuente: El autor

8.1.13 Continuidad de seguridad de la información.

A continuación se presenta los resultados obtenidos para el Dominio A.17 Continuidad de Seguridad de la Información en donde se muestra el promedio por control, dominio, y los principales hallazgos y recomendaciones:

Tabla 15: Continuidad de seguridad de la información

A.17	CONTINUIDAD DEL NEGOCIO	PROMEDIO POR DOMINIO	5%	PRINCIPALES HALLAZGOS Y RECOMENDACIONES
A.17.1	Continuidad de Seguridad de la información	Promedio por control	10%	Con base en la información obtenida durante las entrevistas, se pudo constatar que IMN no cuenta con un Plan de Continuidad del Negocio o un Plan de Recuperación de Desastres. La continuidad de la seguridad de la información debe estar incluida en estos planes. Estos planes deben contar con: análisis de impacto al negocio, análisis de escenario de riesgos, definición de estrategias de continuidad, pruebas, auditorias, entrenamiento y mejora continua.
A.17.1.1	Planificación de la continuidad de la seguridad de la información	% por control	20%	
A.17.1.2	Implementación de la continuidad de la seguridad de la información	% por control	20%	
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	% por control	0%	
A.17.2	Redundancias	Promedio por control	0%	
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	% por control	0%	

Fuente: El autor

8.1.14 Cumplimiento.

A continuación se presenta los resultados obtenidos para el Dominio A.18 Cumplimiento en donde se muestra el promedio por control, dominio, y los principales hallazgos y recomendaciones:

Tabla 16: Cumplimiento

A.18	CUMPLIMIENTO	PROMEDIO POR DOMINIO	21%	PRINCIPALES HALLAZGOS Y RECOMENDACIONES
A.18.1	**Cumplimiento de los requisitos legales**	**Promedio por control**	36%	Según el numeral 15.2 del documento POLITICA DE SEGURIDAD DE LA INFORMACION en donde establece que: "El IMN debe cumplir con la reglamentación de propiedad intelectual vigente en el país y ejecutará revisiones periódicas para asegurar que estén respetando los derechos de propiedad intelectual. Los derechos de propiedad intelectual incluyen licencias de códigos fuentes que hagan parte de desarrollos internos de software, documentos generados como parte del conocimiento del negocio de IMN, propuestas comerciales, patentes, información publicitaria y comercial que involucre la imagen corporativa del IMN", se puede constatar el compromiso de IMN con la protección de los derechos de propiedad intelectual. Adicionalmente se recomienda contar con una Política para la protección y privacidad de información de datos personales de acuerdo a la legislación vigente. Finalmente se deben realizar auditorías internas o externas sobre seguridad de la información, para verificar el cumplimiento de las políticas de seguridad.
A.18.1.1	**Identificación de la legislación aplicable y requerimientos contractuales**	**% por control**	60%	
A.18.1.2	**Derechos de propiedad intelectual**	**% por control**	60%	
A.18.1.3	**Protección de los registros**	**% por control**	20%	
A.18.1.4	**Protección de los datos y privacidad de la información personal**	**% por control**	20%	
A.18.1.5	**Regulación de los controles criptográficos**	**% por control**	20%	
A.18.2	**Revisiones de seguridad de la información**	**Promedio por control**	7%	
A.18.2.1	**Revisión independiente de la seguridad de la información**	**% por control**	0%	
A.18.2.2	**Cumplimiento con las políticas y las normas de seguridad**	**% por control**	0%	
A.18.2.3	**Verificación del cumplimiento técnico**	**% por control**	20%	

Fuente: El autor

8.2 CONSOLIDADO DE RESULTADOS DEL ANÁLISIS DE MADUREZ

A continuación se presenta en las siguientes ilustraciones los resultados del análisis de brecha. Para realizarlo se hicieron 5 preguntas por cada control, cada una contribuyendo con un 20%. Estos valores fueron sumados para obtener el nivel de madurez del control de acuerdo a la Tabla No. 2. Para obtener el nivel de madurez por dominio se promediaron los resultados obtenidos por control. Finalmente, para obtener el nivel de madurez para todos los dominios se promediaron los resultados por dominio y para las cláusulas se promediaron los resultados obtenidos por cláusula.

El promedio del dominio expresa cómo está la gestión de la seguridad de la información. El nivel Optimizado corresponde a un mayor nivel de madurez y en el otro extremo contrapuesto se encuentra el nivel Inexistente, lo que quiere decir que el nivel de cumplimiento y la madurez en este control debe mejorarse con un nivel más alto de prioridad una vez se inicie la implementación de los controles de seguridad dentro del Sistema de Gestión de la Seguridad de la Información. Por cada dominio de la NTC/ISO 27001:2013 se debe determinar cuáles controles se van implementar y a qué nivel de cumplimiento queremos llegar en un tiempo razonable. La seguridad de la información no es un producto sino más bien un proceso continuo que debe integrarse dentro del instituto para garantizar la confidencialidad, la integridad y la disponibilidad de la información. La información es uno de los activos más importantes para poder cumplir con la misión organizacional.

8.2.1 Nivel de madurez por Cláusulas.

Los requisitos establecidos en la norma NTC/ISO 27001:2013 son genéricos y están previstos para ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza. Considerando que el IMN declara conformidad con esta norma, la evaluación y análisis de brechas se hizo frente a cada requisito especificado en los numerales 4 al 10, puesto que no es aceptable excluir ninguno de ellos.

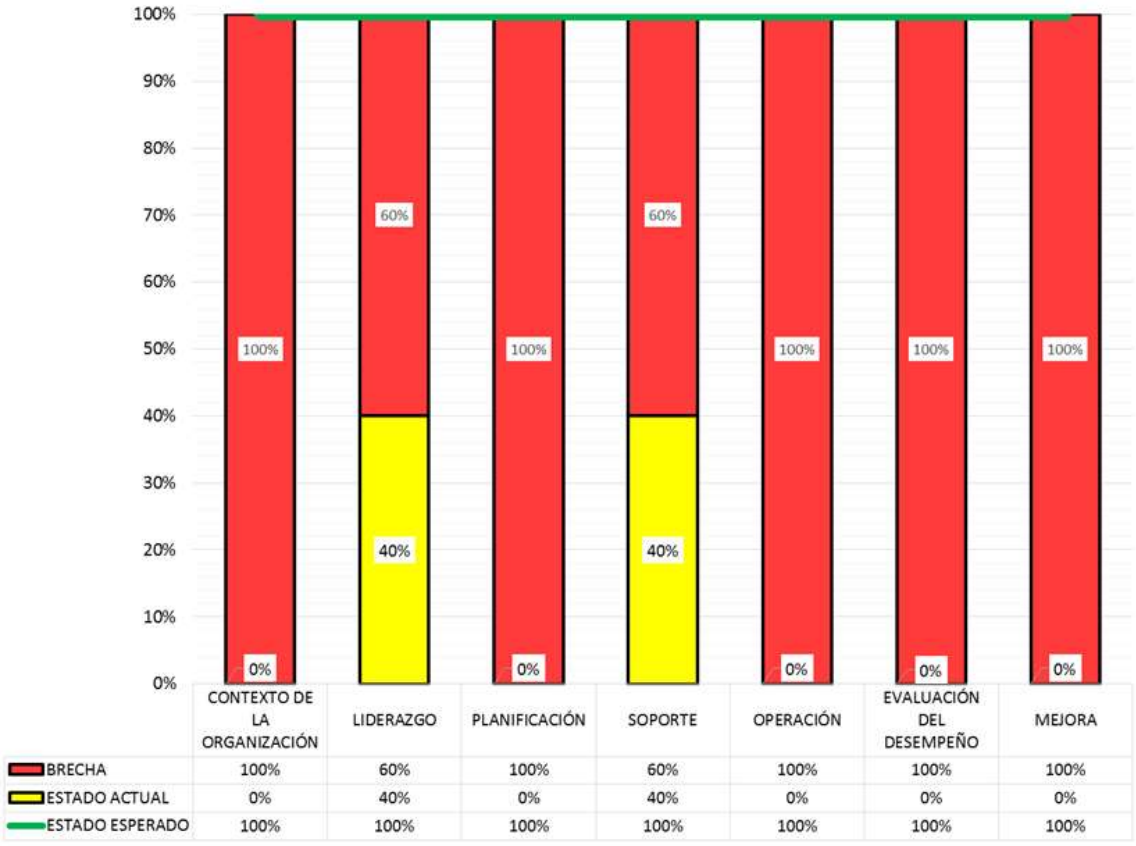
Seguidamente, se presenta el grado actual de implementación y cumplimiento del Instituto frente a las cláusulas.

Figura 6: Resultados por cláusula

NUMERAL	CLAUSULA	ESTADO ACTUAL	BRECHA	ESTADO ESPERADO	NIVEL
4	CONTEXTO DE LA ORGANIZACIÓN	0%	100%	100%	Inexistente
5	LIDERAZGO	40%	60%	100%	Repetible
6	PLANIFICACIÓN	0%	100%	100%	Inexistente
7	SOPORTE	40%	60%	100%	Repetible
8	OPERACIÓN	0%	100%	100%	Inexistente
9	EVALUACIÓN DEL DESEMPEÑO	0%	100%	100%	Inexistente
10	MEJORA	0%	100%	100%	Inexistente
PROMEDIO CLAUSULAS		11%			Inicial

Fuente: El autor

Grafica 1: Resultados por cláusula



Fuente: El autor

Analizando el gráfico, se evidencia que las cláusulas Liderazgo y Soporte, presentan un nivel de madurez del 40% cada una, es decir, se ubican en un estado Repetible, contrario a las demás cláusulas que presentan un nivel de madurez Inexistente, no

obstante, todas se ubican por debajo del estado esperado Optimizado, lo que indica que requieren una intervención inmediata sí el objetivo es la implementación completa del SGSI.

Finalmente, del promedio de las cláusulas se obtiene el resultado del 11% con un nivel de madurez Inicial.

8.2.2 Nivel de madurez por dominios

Continuando con el análisis de brechas, se tomó como referencia la norma NTC/ISO 27001:2013, compuesto por 14 dominios y 114 controles, los cuales fueron analizados en detalle con las condiciones actuales del IMN.

Seguidamente, se presenta el grado actual de implementación y cumplimiento del Instituto frente a los 14 dominios.

Figura 7: Resultados por dominio

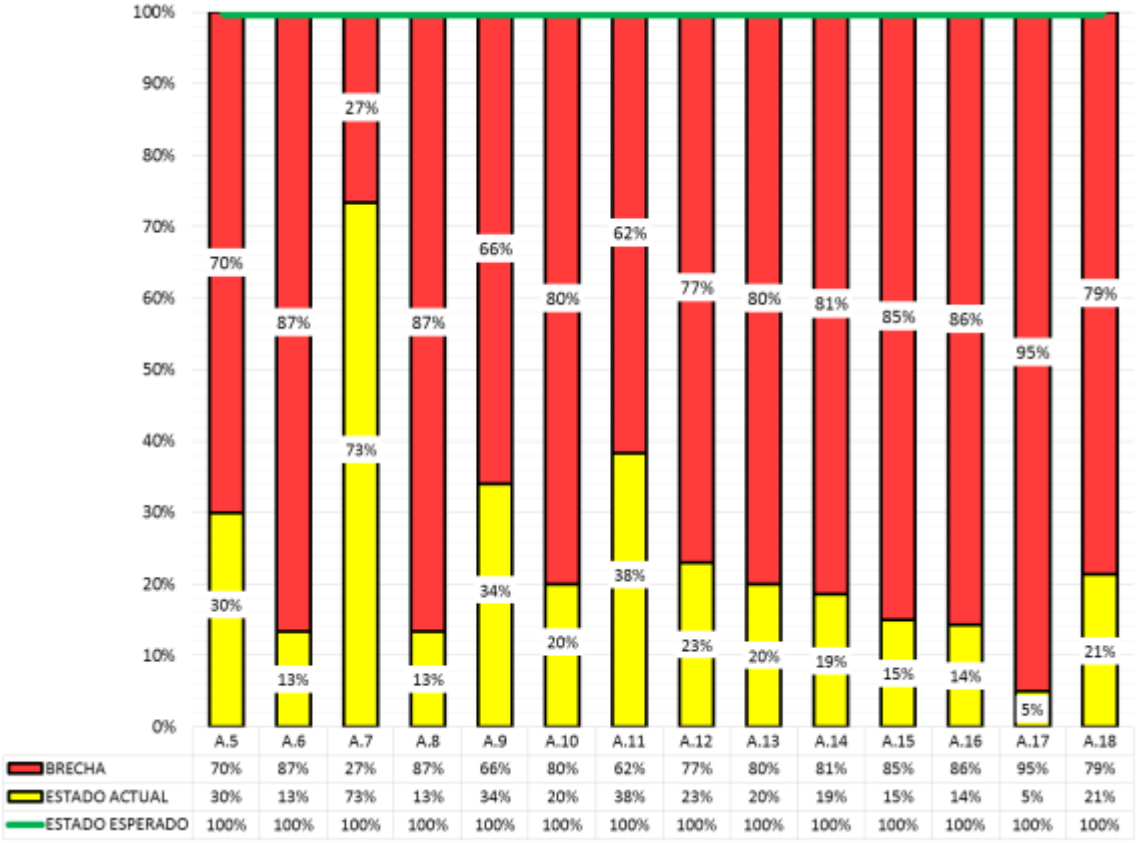
NUMERAL	CLAUSULA	ESTADO ACTUAL	BRECHA	ESTADO ESPERADO	NIVEL
A.5	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	30%	70%	100%	Repetible
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	13%	87%	100%	Inicial
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	73%	27%	100%	Administrado
A.8	GESTIÓN DE ACTIVOS	13%	87%	100%	Inicial
A.9	CONTROL DE ACCESO	34%	66%	100%	Repetible
A.10	CRIPTOGRAFÍA	20%	80%	100%	Inicial
A.11	SEGURIDAD FÍSICA	38%	62%	100%	Repetible
A.12	GESTIÓN DE OPERACIONES	23%	77%	100%	Repetible
A.13	SEGURIDAD DE LAS COMUNICACIONES	20%	80%	100%	Inicial
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	19%	81%	100%	Inicial
A.15	RELACIONES CON LOS PROVEEDORES	15%	85%	100%	Inicial
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	14%	86%	100%	Inicial
A.17	CONTINUIDAD DE SEGURIDAD DE LA INFORMACION	5%	95%	100%	Inicial
A.18	CUMPLIMIENTO	21%	79%	100%	Repetible
PROMEDIO CLAUSULAS		24%			Repetible

Fuente: El autor

Analizando el siguiente gráfico, se puede observar que el dominio con mayor nivel de madurez es el A.7 Seguridad de los recursos humanos (Administrado), seguido de A.11 Seguridad física (Repetible), A.9 Control de acceso (Repetible) y A.5

Política de seguridad de la información (Repetible). Los demás dominios se encuentran por debajo del 24% que corresponde a un estado Repetible.

Grafica 2: Resultados por dominio

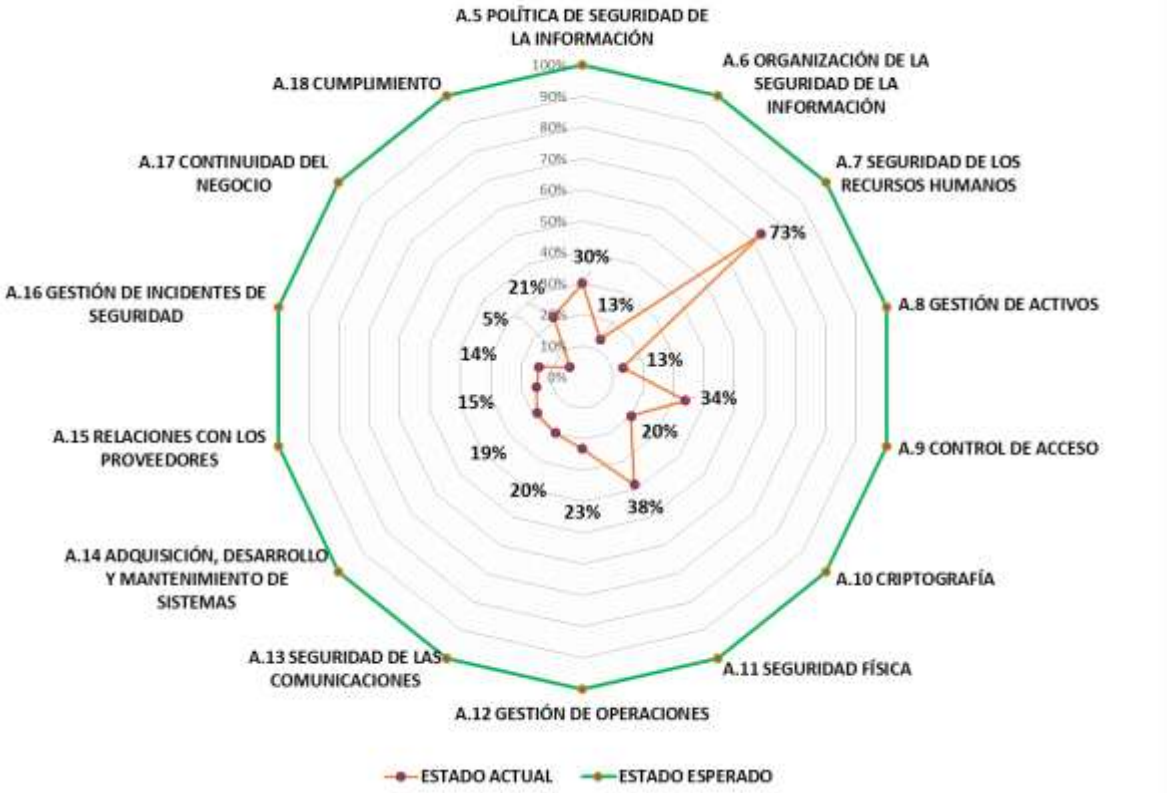


	A.5	A.6	A.7	A.8	A.9	A.10	A.11	A.12	A.13	A.14	A.15	A.16	A.17	A.18
BRECHA	70%	87%	27%	87%	66%	80%	62%	77%	80%	81%	85%	86%	95%	79%
ESTADO ACTUAL	30%	13%	73%	13%	34%	20%	38%	23%	20%	19%	15%	14%	5%	21%
ESTADO ESPERADO	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

Fuente: El autor

A continuación se presenta el diagrama tipo radar en donde se puede identificar la brecha existente con relación a los 14 dominios y 114 controles, los cuales fueron analizados en detalle con las condiciones actuales del IMN:

Grafica 3: Radar por dominio



Fuente: El autor

Analizando el gráfico, se puede observar que el dominio con mayor nivel de madurez es el A.7 Seguridad de los recursos humanos (Administrado). Seguido de A.11 Seguridad física (Repetible), A.9 Control de acceso (Repetible) y A.5 Política de seguridad de la información (Repetible).

Los demás dominios se encuentran por debajo del 24% que corresponde a un estado Repetible.

8.3 PRINCIPALES HALLAZGOS Y RECOMENDACIONES

Teniendo en cuenta los dominios con menor nivel de madurez, se considera importante que éstos sean tratados con mayor prioridad, por esta razón, a continuación presentamos los principales hallazgos y recomendaciones frente a estos dominios:

Figura 8: Dominios en estado inicial

NUMERAL	CLAUSULA	ESTADO ACTUAL	BRECHA	ESTADO ESPERADO	NIVEL
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	13%	87%	100%	Inicial
A.8	GESTIÓN DE ACTIVOS	13%	87%	100%	Inicial
A.10	CRIPTOGRAFÍA	20%	80%	100%	Inicial
A.13	SEGURIDAD DE LAS COMUNICACIONES	20%	80%	100%	Inicial
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	19%	81%	100%	Inicial
A.15	RELACIONES CON LOS PROVEEDORES	15%	85%	100%	Inicial
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	14%	86%	100%	Inicial
A.17	CONTINUIDAD DE SEGURIDAD DE LA INFORMACION	5%	95%	100%	Inicial

Fuente: El autor

8.3.1 Cláusulas.

Para la implementación del SGSI se recomienda:

• Entender claramente el contexto del instituto frente a seguridad de la información.

• Contar con el apoyo de la alta dirección para la implementación del SGSI.

• Implementar un proceso de gestión de riesgos sobre los activos de información.

• Establecer los objetivos de seguridad de la información.

• Implementar un procedimiento de auditorías internas en seguridad de la información.

• Implementar un procedimiento para el tratamiento de no conformidades y acciones correctivas relacionadas con seguridad de la información.

• Establecer indicadores para medir el desempeño de la seguridad de la información y la eficacia del SGSI.

8.3.2 Organización de la seguridad de la información.

Actualmente, los roles y responsabilidades de seguridad de la información están en cabeza de la Oficina de Tecnologías de la Información, no obstante, es recomendable que esta oficina tenga el apoyo, la colaboración y la suficiencia de recursos desde la alta dirección.

EL departamento de sistemas informático u oficina de tecnología de la información OTI del Instituto Museo Nacional IMN; está conformada por 5 áreas especializadas con cada uno de sus profesionales responsables en cabeza del Jefe nacional, como se describe a continuación:

Tabla 17: Descripción de roles y responsabilidades

ROLES Y RESPONSABILIDADES	
Jefe OTI	
Perfil profesional	Ingeniero de sistemas, Maestría en telecomunicaciones
Capacidades y principios	Persona altamente capacitada por sus estudios y con buenos principios morales y éticos, conforme a los principios vigentes en nuestra sociedad y al código de ética del ingeniero de sistemas.
1. Infraestructura Y Comunicaciones.	
Líder	
Perfil profesional	Especialización en telecomunicaciones, ingeniero de sistemas, 10 años de experiencia en administración de redes.
Capacidades y principios	Persona altamente capacitada por sus estudios y con buenos principios morales y éticos, conforme a los principios vigentes en nuestra sociedad y al código de ética del ingeniero de sistemas.
Nivel de acceso a la información	a.) Realiza tareas técnicas relacionadas con el diseño y la instalación, mantenimiento de la plataforma de redes y comunicación. b.)Implementa los controles definidos en las políticas de seguridad de la información. c.)Garantiza la disponibilidad de los servicios: sistemas de información, correo electrónico, internet, voz ip, datos a través de la red corporativa. d.)Administrar los elementos y servicios que conforman la infraestructura tecnológica con un equipo de trabajo que atiende las líneas de servicios.

Tabla 17 (Continuación)

2. Sistema De Información	
Líder:	
Perfil profesional	Especialización en gestión de proyectos, ingeniero de sistemas, trece años de experiencia en gestión informática.
Capacidades y principios	Persona altamente capacitada por sus estudios y con buenos principios morales y éticos, conforme a los principios vigentes en nuestra sociedad y al código de ética del ingeniero de sistemas.
Nivel de acceso a la información	La gestión y el seguimiento de las operaciones diarias se generan y procesan a través de los sistemas de información, que facilitan el registro de las operaciones en las diferentes etapas de los procesos estratégicos, misionales y de apoyo. b.) Los sistemas de información son herramientas fundamentales para desarrollo del IMN; ya que permiten la sistematización y automatización de los procesos en diferentes áreas, lo que trae ventajas competitivas sostenibles en el tiempo. c.)Desarrollar las actividades diarias de forma eficiente en el menor tiempo posible y que los resultados se reflejen en los indicadores de gestión. d.)Los sistemas de información están compuesta por diferentes aplicaciones.
3. Administración Y Desarrollo Tecnológico	
Líder:	
Perfil profesional	Especialización en Administración de recursos tecnológicos, ingeniero de sistemas, 20 años de experiencia en administración informática.
Capacidades y principios	Persona altamente capacitada por sus estudios y con buenos principios morales y éticos, conforme a los principios vigentes en nuestra sociedad y al código de ética del ingeniero de sistemas.

Tabla 17 (Continuación)

Nivel de acceso a la información	Evaluar la infraestructura tecnológica del instituto u proponer procesos de modernización tecnológica apropiados. b.) Aprovechar las tendencias tecnológicas para el beneficio de la entidad. c.)Generar proyectos de tecnología asegurando la efectividad recepción, la apropiación y la transferencia de tecnología. e.)Evaluar y asesorar proyectos de tecnología desde la perspectiva estratégica financiera. f.)Asesorar proyectos de modernización tecnológica y de implementación de sistemas de información gerencial.
1. Mesa De Ayuda	
Líder:	
Perfil profesional	Especialización Soporte tecnológico, ingeniero de sistemas, 8 años de experiencia en administración de soporte tecnológico.
Capacidades y principios	Persona altamente capacitada por sus estudios y con buenos principios morales y éticos, conforme a los principios vigentes en nuestra sociedad y al código de ética del ingeniero de sistemas.
Nivel de acceso a la información	Es un conjunto de recursos tecnológicos y humanos diseñados para atender y solucionar los requerimientos e incidentes reportados por los usuarios ocasionados por los diferentes agentes que intervienen en los servicios de infraestructura tecnológica. b.) El personal encargado de la mesa de ayuda proporciona respuestas y soluciones a los usuarios finales, clientes o beneficiarios en productos y servicios. e.) La mesa de ayuda proporciona el soporte a través de registro en línea (Discovery), el correo electrónico o la llamada telefónica.

Autor: Instituto Museo Nacional

La asignación de las responsabilidades de seguridad de la información se debería mencionar desde las políticas de la seguridad de la información. Dentro de las responsabilidades por definir se deben considerar las de los usuarios de los activos de TI, los propietarios, los custodios, los dueños de los riesgos de seguridad de la información y terceras partes con acceso a los activos de información.

Adicionalmente, se recomienda nombrar formalmente un gerente u oficial de seguridad de la información, a través del Departamento Administrativo de la función pública, que asuma la responsabilidad de todos los procesos definidos en el alcance y que la obtención de recursos y la implementación de controles con frecuencia estarán a cargo de los directores individuales.

El gerente u oficial de seguridad de la información y su equipo de trabajo a apoyo deben ser competentes en el área y se les deben brindar oportunidades para mantenerse actualizados con los avances en este tema. El equipo de trabajo deberá estar conformado por profesionales con conocimientos en las leyes, tecnología y personal especializado en seguridad informática.

Es importante también, que exista una política sobre el uso de dispositivos móviles con el fin de evitar posibles riesgos de seguridad de la información que puedan impactar la reputación del instituto.

8.3.3 Gestión de Activos.

Se evidenció durante las entrevistas que el instituto cuenta con un inventario de bienes e inmuebles bastante maduro, aunque éste no contempla activos de seguridad de la información, lo que conlleva a la ausencia de un sistema de clasificación y etiquetado de la información.
Se recomienda contar con política y procedimientos para el borrado y destrucción de los medios.

8.3.4 Criptografía.

Se recomienda contar con una Política de uso de controles criptográficos, la cual sea aplicada siguiendo las normas vigentes nacionales, teniendo en cuenta los niveles de confidencialidad de la información y que los algoritmos utilizados sean seguros.

8.3.5 Gestión de Operaciones.

Las políticas y los procedimientos son parte fundamental de un modelo de seguridad. Los procedimientos permiten realizar ciertas actividades de manera

segura, estos deben estar revisados, aprobados, publicados, comunicados y socializados, para asegurar su adecuada utilización.
Por otra parte, la gestión de cambios debe estar soportada por políticas y procedimientos, y debe contemplar los riesgos asociados al cambio.
Así mismo, el registro de todos los eventos es importante para la gestión de los incidentes de seguridad.
Finalmente a todos los sistemas se les debe realizar un análisis de vulnerabilidad al menos una vez al año acompañado de un plan de remediación.

8.3.6 Seguridad en las Comunicaciones.

Se deben tener políticas y procedimientos para la transferencia de información a otras entidades.

Los elementos de red deben enviar sus registros a un servidor centralizado y deben existir estándares de configuración seguros.

8.3.7 Adquisición, Desarrollo y Mantenimiento de Sistemas.

La seguridad de la información debe ser considerada en todo el ciclo de desarrollo (SDLC). Es recomendable contar con políticas y procedimientos para el desarrollo seguro, junto con herramientas de software que permitan la identificación de líneas de código inseguro.

Finalmente el entrenamiento, la educación y la sensibilización en seguridad de la información deben ser impartidas de manera formal a todos los desarrolladores.

8.3.8 Relaciones con los Proveedores.

Se debe contar con una política, procedimientos, formatos y guías para gestionar la relación con los proveedores en cuanto a la seguridad de la información. Los contratos con los proveedores deben establecer cláusulas para el cuidado de la información. La ejecución de estos contratos debe ser supervisada para garantizar la confidencialidad, disponibilidad e integridad y todo cambio al contrato debe considerar los riesgos asociados a la información.

8.3.9 Gestión de Incidentes de Seguridad de la Información.

Para lograr una gestión consistente y efectiva de los incidentes de seguridad de la información se deben establecer: por un lado, asignación de responsabilidades y por el otro, procedimientos detallados para clasificar, dar respuesta, escalamiento, solución, aprendizaje y registro de estos incidentes. Se recomienda realizar un programa de socialización a funcionarios, contratistas y proveedores, para que reporten eventos de seguridad a la mayor brevedad posible.

8.3.10 Continuidad de la Seguridad de la Información.

Con base en la información obtenida durante las entrevistas, se pudo constatar que IMN no cuenta con un Plan de Continuidad del Negocio o un Plan de Recuperación de Desastres. La continuidad de la seguridad de la información debe estar incluida en estos planes. Estos planes deben contar con: análisis de impacto al negocio, análisis de escenario de riesgos, definición de estrategias de continuidad, pruebas, auditorias, entrenamiento y mejora continua.

8.3.11 Cumplimiento.

Según el numeral 15.2 del documento POLITICA DE SEGURIDAD DE LA INFORMACION en donde establece que: "El IMN debe cumplir con la reglamentación de propiedad intelectual vigente en el país y ejecutará revisiones periódicas para asegurar que estén respetando los derechos de propiedad intelectual. Los derechos de propiedad intelectual incluyen licencias de códigos fuentes que hagan parte de desarrollos internos de software, documentos generados como parte del conocimiento del negocio de IMN, propuestas comerciales, patentes, información publicitaria y comercial que involucre la imagen corporativa del IMN", se puede constatar el compromiso de IMN con la protección de los derechos de propiedad intelectual.

Adicionalmente se recomienda contar con una Política para la protección y privacidad de información de datos personales de acuerdo a la legislación vigente.

Finalmente se deben realizar auditorías internas o externas sobre seguridad de la información, para verificar el cumplimiento de las políticas de seguridad.

8.3.12 Establecimiento del plan estratégico de seguridad de la información.

Tanto para el Instituto Museo Nacional como para otras entidades del estado, la seguridad de la información en sus etapas tempranas, se ha centrado en la protección de la tecnología de la información orientada a servicios de procesamientos y almacenamiento, más que a la información en sí misma, que es a lo que se le denomina seguridad informática.

Para el caso del Instituto en lo que respecta al diagnóstico para determinar el nivel de seguridad de la información es necesario extender el alcance centrado en la tecnología y apuntar a una seguridad integral, más allá de la aplicación de las políticas y los controles de seguridad en la que se proteja la información, sin importar cómo se maneja, procesa o almacena.

Con este objetivo se sugiere desarrollar un plan estratégico de seguridad de la información (PESI) que permita identificar el portafolio de proyectos que deben ser desarrollados por el IMN y asignar el presupuesto anual de manera priorizada con miras a propender que los riesgos de la información sean administrados

apropiadamente. Igualmente, se deben identificar los requerimientos del MSPI, alineado con las mejores prácticas, estándares y objetivos del negocio.

El PESI debe definirse y priorizarse teniendo en cuenta, entre otras cosa lo siguiente:

8.3.13 Objetivos estratégicos del instituto.

La gestión de los riegos, que se clasifican de acuerdo con su responsabilidad e impacto, para mitigarlos y reducir sus potenciales impactos a niveles aceptables. La optimización de los recursos, que utilice el conocimiento en seguridad y, de forma eficiente y efectiva, la infraestructura existente.

8.3.14 Implementación de una herramienta para gestionar el sgsi.

Se recomienda la adquisición e implementación de una herramienta automatizada que apoye el cumplimiento de todos los requisitos del SGSI, para esto se manejó el ciclo PHVA el cual permite su integración con otros sistemas de gestión (por ejemplo, ISO 9001) Se sugiere tener en cuenta entre otros los siguientes requisitos para la selección de la herramienta:

- Gestión documental
- Definición de objetivos y métricas
- Gestión de Activos
- Seguimientos a controles
- Actualización y seguimientos a los planes de tratamientos de riesgo
- Seguimiento a planes de capacitación
- Seguimiento a auditorías internas
- Seguimiento a las revisiones de la dirección
- Seguimiento a acciones correctivas y preventivas
- Gestión de incidentes

Para dar cumplimiento a este objetivo específico como fase previa a la implementación de un modelo de seguridad y privacidad de la información MSPI se utilizaron los siguientes mecanismos de recolección de información:

Entrevista, consultas, observaciones, revisión de documentación.

8.4 EVALUACIÓN DE APLICABILIDAD

Seguidamente se realiza un análisis de aplicación teniendo en cuenta los 14 dominios, 35 objetivos de control con los 114 controles de la ISO 27001:2013.

Tabla 18: Evaluación de aplicabilidad con objetivo de control por dominio

DOMINIO	OBEJTIVO DE CONTROL		APLICA	OBS
POLITICA DE SEGURIDAD	5.1	Directrices de la dirección en seguridad de la información.	SI	
	5.1.1	Conjunto de políticas para la seguridad de la información.	SI	
	5.1.2	Revisión de las políticas para la seguridad de la información.	SI	
ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION	6.1	Organización Interna.	SI	
	6.1.1	Asignación de responsabilidades para la seguridad de la información.	SI	
	6.1.2	Segregación de tareas.	SI	
	6.1.3	Contacto con las autoridades.	SI	
	6.1.4	Contacto con grupo de interés especial.	SI	
	6.1.5	Seguridad de la información en la gestión de proyecto.	SI	
	6.2	Dispositivos Móviles y trabajo remoto.	SI	
	6.2.1	Políticas de los dispositivos móviles.	SI	
	6.2.2	Trabajo remoto.	SI	
SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	7.1	Antes de la contratación.	SI	
	7.1.1	Investigación de antecedentes.	SI	
	7.1.2	Términos y condiciones de contratación.	SI	
	7.2	Durante la contratación.	SI	
	7.2.1	Responsabilidades de gestión.	SI	
	7.2.2	Concientización, educación y formación en seguridad de la información.	SI	
	7.2.3	Proceso disciplinario.	SI	
	7.3	Desvinculación y cambio de empleo.	SI	
	7.3.1	Responsabilidades en la desvinculación o cambio de empleo.	SI	

Tabla 18. (Continuación)

DOMINIO	OBEJTIVO DE CONTROL		APLICA	OBS
ADMINISTRACIÓN DE ACTIVOS	8.1	Responsabilidades de los activos	SI	
	8.1.1	Inventarios de activos.	SI	
	8.1.2	Propiedad de los activos.	SI	
	8.1.3	Uso aceptable de los activos.	SI	
	8.1.4	Devolución de activos.	SI	
	8.2	Clasificación de la información.	SI	
	8.2.1	Directrices de la clasificación.	SI	
	8.2.2	Etiquetado y manipulado de la información	SI	
	8.2.3	Manipulación de activos	SI	
	8.3	Manejo de los soportes de almacenamiento	SI	
	8.3.1	Gestión de soportes extraíbles	SI	
	8.3.2	Eliminación de soportes	SI	
	8.3.3	Soportes físicos en tránsito.	SI	
CONTROL DE ACCESO	9.1	Requisitos del negocio para el control de accesos.	SI	
	9.1.1	Políticas de control de accesos.	SI	
	9.1.2	Control de acceso a las redes y servicios asociados.	SI	
	9.2	Gestión de acceso de usuario	SI	
	9.2.1	Gestión de altas/bajas en el registro de usuarios	SI	
	9.2.2	Gestión de los derechos de acceso asignados a usuarios.	SI	
	9.2.3	Gestión de los derechos de acceso con privilegios especiales	SI	
	9.2.4	Gestión de información confidencial de autenticación de usuario	SI	
	9.2.5	Revisión de los derechos de acceso de los usuarios	SI	
	9.2.6	Retirada o adaptación de los derechos de acceso	SI	
	9.3	Responsabilidades del usuario	SI	
	9.3.1	Uso de información confidencial para la autenticación.	SI	

Tabla 18. (Continuación)

DOMINIO	OBEJTIVO DE CONTROL		APLICA	OBS
	9.4	Control de acceso a sistemas y aplicaciones.	SI	
	9.4.1	Restricción del acceso a la información.	SI	
	9.4.2	Procedimientos seguros de inicio de sesión.	SI	
	9.4.3	Gestión de contraseña de usuario.	SI	
	9.4.4	Uso de herramientas de administración de sistemas.	SI	
	9.4.5	Control de acceso al código fuente de los programas.	SI	
CRIPTOGRAFÍA	10.1	Controles criptográficos.	SI	
	10.1.1	Políticas de uso de los controles criptográficos.	SI	
	10.1.2	Gestión de claves.	SI	
SEGURIDAD FISICA Y AMBIENTAL	11.1	Áreas seguras.	SI	
	11.1.1	Perímetro de seguridad física.	SI	
	11.1.2	Controles físicos de entrada	SI	
	11.1.3	Seguridad de oficinas, despachos y recursos.	SI	
	11.1.4	Protección contra las amenazas externas y ambientales.	SI	
	11.1.5	El trabajo en áreas seguras.	SI	
	11.1.6	Áreas de acceso público, carga y descarga.	SI	
	11.2	Seguridad de los equipos.	SI	
	11.2.1	Emplazamiento y protección de equipos.	SI	
	11.2.2	Instalaciones de suministro.	SI	
	11.2.3	Seguridad del cableado.	SI	
	11.2.4	Mantenimiento de los equipos.	SI	
	11.2.5	Salida de activos fuera de las dependencias.	SI	
	11.2.6	Seguridad de los y activos fuera de las instalaciones.	SI	
	11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento.	SI	
	11.2.8	Equipo informático de usuario desentendido.	SI	
	11.2.9	Política de puesto de trabajo despejado.	SI	

Tabla 18. (Continuación)

DOMINIO	OBJETIVO DE CONTROL		APLICA	OSB
SEGURIDAD DE LAS OPERACIONES	12.1	Procedimientos operacionales y responsabilidades.	SI	
	12.1.1	Documentación de procedimientos de operaciones.	SI	
	12.1.2	Gestión de cambios.	SI	
	12.1.3	Gestión de capacidades.	SI	
	12.1.4	Separación de entornos de desarrollo, prueba y producción.	SI	
	12.2	Protección contra el código malicioso.	SI	
	12.2.1	Controles central el código malicioso.	SI	
	12.3	Copias de seguridad.	SI	
	12.3.1	Copias de seguridad de la información.	SI	
	12.4	Registro de actividad y supervisión.	SI	
	12.4.1	Registro y gestión de eventos de actividad.	SI	
	12.4.2	Protección de los registro de información.	SI	
	12.4.3	Registro de actividad del administrador y operador del sistema.	SI	
	12.4.4	Sincronización de relojes.	SI	
	12.5	Control del software en explotación.	SI	
	12.5.1	Instalación del software en sistemas en producción.	SI	
	12.6	Gestión de la vulnerabilidad técnica.	SI	
	12.6.1	Gestión de las vulnerabilidades técnicas.	SI	
	12.6.2	Restricciones en la instalación de software.	SI	
	12.7	Consideraciones de las auditorias de los sistemas de información.	SI	
	12.7.1	Controles de auditoria de los sistemas de información.	SI	

Tabla 18. (Continuación)

DOMINIO	OBJETIVOS DE CONTROL		APLICA	OBS
SEGURIDAD EN LAS TELECOMUNICACIONES	13.1	Gestión de la seguridad en las redes.	SI	
	13.1.1	Control de red.	SI	
	13.1.2	Mecanismos de seguridad asociados a servicios en red	SI	
	13.1.3	Segregación de redes.	SI	
	13.2	Protección contra código malicioso.	SI	
	13.2.1	Políticas y procedimientos de intercambio de información.	SI	
	13.2.2	Acuerdos de intercambio.	SI	
	13.2.3	Mensajería electrónica	SI	
	13.2.4	Acuerdos de confidencialidad y secreto.	SI	
ADQUISICION, DESARROLLO Y MANTENIMIENTO DEL SISTEMA	14.1	Requisitos de seguridad de los sistemas de información.	SI	
	14.1.1	Análisis y especificación de los requisitos de seguridad.	SI	
	14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas.	SI	
	14.1.3	Protección de las transacciones por redes telemáticas.	SI	
	14.2	Seguridad en los procesos de desarrollo y soporte.	SI	
	14.2.1	Política de desarrollo seguro	SI	
	14.2.2	Procedimientos de control de cambios en los sistemas.	SI	
	14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	SI	
	14.2.4	Restricciones a los cambios en los paquetes de software.	SI	
	14.2.5	Uso de principios de ingeniera en protección de sistemas.	SI	
	14.2.6	Seguridad en entornos de desarrollo.	SI	
	14.2.7	Externalización del desarrollo de software.	SI	
	14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas.	SI	
	14.2.9	Pruebas de aceptación.	SI	
	14.3	Datos de prueba.	SI	
	14.3.1	Protección de datos utilizados en pruebas.	SI	

Tabla 18. (Continuación)

DOMINIO	OBJETIVO DE CONTROL		APLICA	OBS
RELACION CON PROVEEDORES	15.1	Seguridad de la información en las relaciones con el proveedor.	SI	
	15.1.1	Política de seguridad de la información para las relaciones con los proveedores.	SI	
	15.1.2	Abordar la seguridad dentro de los acuerdos del proveedor.	SI	
	15.1.3	Cadena de suministro de tecnologías de la información y comunicaciones	SI	
	15.2	Gestión de entrega del servicio del proveedor.	SI	
	15.2.1	Supervisor y revisión de los servicios de los servicios del proveedor.	SI	
	15.2.2	Gestión de cambios a los servicios del proveedor.	SI	
GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION	16.1	Gestión de incidentes de seguridad de la información y mejoras.	SI	
	16.1.1	Responsabilidades y procedimientos.	SI	
	16.1.2	Notificación de los eventos de seguridad.	SI	
	16.1.3	Notificación de puntos débiles de la seguridad.	SI	
	16.1.4	Valoración de eventos de la seguridad de la información y decisiones	SI	
	16.1.5	Respuestas a los incidentes de seguridad	SI	
	16.1.6	Aprendizaje de los incidentes de seguridad	SI	
	16.1.7	Recopilación de evidencia.	SI	
ASPECTOS DE SEGURIDAD EN LA GESTIÓN DE LA CONTINBUIDAD DEL NEGOCIO	17.1	Continuidad de la seguridad de la información.	SI	
	17.1.1	Planificación de la continuidad de la seguridad de la información	SI	
	17.1.2	Implantación de la continuidad de la seguridad de la información.	SI	
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	SI	
	17.2	Redundancias.	SI	
	17.2.1	Disponibilidad de instalaciones para el procesamiento de la información.	SI	

Tabla 18. (Continuación)

DOMINIO	OBJETIVO DE CONTROL		APLICA	OBSB
CUMPLIMIENTO	18.1.2	Derechos de propiedad intelectual (DPI)	SI	
	18.1.3	Protección de los registros de la organización.	SI	
	18.1.4	Protección de datos y privacidad de la información personal.	SI	
	18.1.5	Regulación de los controles criptográficos.	SI	
	18.2	Revisiones de la seguridad de la información.	SI	
	18.2.1	Revisión independiente de la seguridad de la información.	SI	
	18.2.2	Cumplimiento de las políticas y normas de seguridad.	SI	
	18.2.3	Comprobación del cumplimiento.	SI	

Fuente: El autor

8.5 CRITERIOS DE EVALUACIÓN

La siguiente plantilla de evaluación está basada en los 14 dominios, 35 objetivos de control y 124 controles de la ISO 27001 del 2013.

Con esta plantilla se evalúan los tres siguientes aspectos básicos:

I. Si el control existe.
II. Determinar cuál sería el nivel de formalización e implementación.
III. Si se realiza el seguimiento y/o monitoreo a los controles.

Se especifican aspectos y definiciones que pueden ser diligenciados en cada campo de la plantilla.

Tabla 19: Plantilla criterios de evaluación

CAMPO	DETALLES	POSIBLES RESPUESTAS		
Existencia del control	Responder si el control existe	SI	NO	
Cual	Cuando el control no existe se tiene que describir el motivo.			
Nivel de formalización e implementación	Se describe si el control esta formalizado, divulgado y si hay responsables.	Implementado pero no documentado	Implementado documentado pero no divulgado	Implementado documentado y divulgado
Seguimiento y monitoreo del control	¿Existen indicadores, monitoreo, para ejecución de control.	No existe mecanismo de medición	No existe indicadores de medición, se realiza monitoreo	Si existe indicadores y se realiza monitoreo

Fuente: El autor

8.5.1 Definición de puntajes.

Se determina el puntaje el cual permite definir el promedio como resultado.

Tabla 20: Puntaje de implementación

CAMPO	PUNTAJE
Implementado pero no documentado	1
Implementado documentado pero no divulgado	2
Implementado documentado y divulgado	3

Fuente: El autor

Tabla 21: Puntaje monitoreo de control

CAMPO	PUNTAJE
No existe mecanismo de medición	0
No existe indicadores de medición, se realiza monitoreo	1
Si existe indicadores y se realiza monitoreo	2

Fuente: El autor

8.5.2 Resultados de la evaluación.

La sumatoria de formalización, implementación más la de seguimiento y monitoreo del control, permite concebir el puntaje por cada objetivo de control.

Tabla 22: Resultado de evaluación

ESCALA	CARACTERÍSTICAS
0	No Existe: El instituto no reconoce que existe un problema para solucionar.
1	Inicial: Hay evidencias donde el instituto reconoce que los problemas existen. NO existe un proceso estándar. El enfoque administrativo general
2	Repetible: Los procesos se realizan con procedimientos similares en las distintas áreas donde se aplica la misma actividad. No existe capacitación formal de los procedimientos estándares.
3	Definido: Los procesos estándares están documentado. Se divulgan a través de capacitaciones. El cumplimiento de Los procesos no es de obligatoriedad.
4	Administrador: Cuando los procesos no funcionan de forma objetiva se monitorean pero no se puede medir el cumplimiento de los procedimientos para tomar medidas de cambios.
5	Optimizado: Procesos basados en resultados de mejoras constantes. El cumplimiento de los objetivos se monitorea y se miden los indicadores. La seguridad se administra de forma integral, automatizando el flujo de trabajo.

Fuente: El autor

8.6 ESTRACTIFICACION DE LA ENTIDAD

Dado el abanico de entidades (desde las pequeñas de orden territorial, con bajos presupuestos y ubicadas en zonas remotas del país, hasta las grandes de orden nacional), es necesario definir una escala o "estratificación", que permita definir de antemano un nivel de responsabilidad del instituto, en cuanto a la seguridad de la información. Esta clasificación se enfocará en definir el "nivel" asociado a responsabilidades y requerimientos tecnológicos que deberá cumplir el instituto en cuanto a seguridad de la información.

Para determinar el nivel de estratificación del Instituto Nacional De Museo tomamos como referencia la guía # 2 Estratificación de las entidades públicas versión 2.0.0 MINTIC.

Tabla 23: Escala de Evaluación. Esquema de estratificación de entidades

PARÁMETROS DE CLASIFICACIÓN	RANGOS	PUNTOS
PRESUPUESTO	1. Menos de 3.000 millones de pesos.	3
	2. Entre 3.000 millones y 50.000 millones de pesos.	
	3. Más de 50.000 millones de pesos.	
NÚMERO TOTAL DE COMPUTADORES	1. Menos de 100 computadores.	3
	2. Entre 100 y 500 computadores.	
	3. Más de 500 computadores.	
NÚMERO DE SERVIDORES	1. Menos de 4 Servidores.	2
	2. Entre 4 y 20 Servidores.	
	3. Más de 20 Servidores.	
NÚMERO DE EMPLEADOS DE SISTEMAS (TECNOLOGÍA)	1. Menos de 6 empleados.	2
	2. Entre 6 y 50 empleados.	
	3. Más de 50 empleados.	

Tabla 23. (Continuación)

PARÁMETROS DE CLASIFICACIÓN	RANGOS	PUNTOS
EXISTENCIA Y FUNCIÓN DEL ÁREA DE SISTEMAS (TECNOLOGÍA)	1. No existe un área de sistemas de tecnología de la información o sistemas propiamente.	2
	2. Si Existe un área de tecnología de la información o sistemas propiamente. enfocada en la operación del día a día, que cumple labores en su mayoría REACTIVAS	
	3. Si existe un área de tecnología de la información o sistemas, además de desarrollar funciones del punto anterior, con la planeación y desarrollo de proyectos nuevos o de actualización, administra su propio presupuesto con el desarrollo de labores PROACTIVAS a través de comités y participación en decisiones empresariales.	
EXISTENCIA Y OBJETO DE LA WAN	1. WAN pública (p.ej. Internet) sólo para USAR correo y navegar. Incluye servidores de correo y Web en hosting.	3
	2. WAN pública (p.ej. Internet) con servicios ofrecidos al ciudadano. Puede o no haber desarrollos sofisticados de transaccionalidad.	
	3. Lo anterior más la existencia de una WAN privada (no incluye VPN a través de Internet).	
TRANSACCIONALIDAD EN LA WEB	1. Solo ofrece servicios de consulta (páginas WEB estáticas y correo electrónico)	3
	2. Transaccionalidad local. Generación de servicios y seguimiento de trámites, solo con base en datos y aplicativos propios	
	3. Lo anterior más interacción con aplicativos, datos y servicios de otras entidades y/o terceros.	

Tabla 23. (Continuación)

PARÁMETROS DE CLASIFICACIÓN	RANGOS	PUNTOS
DESARROLLO DE SOFTWARE.	1. No desarrolla software. Incluye aquellas entidades que tienen en hosting una página WEB básica e informativa y un servidor de correo.	3
	2. Sí desarrolla software solo aplicativos internos. Se aclara que este desarrollo puede ser interno o en outsourcing externo.	
	3. Sí desarrolla software para aplicativos externos. Sí publica información transaccional. Puede o no desarrollar software para aplicativos internos. Hay que aclarar que este desarrollo puede ser interno o en outsourcing (realizado por terceros).	

Fuente: El autor

Análisis de los resultados:

Las respuestas fueron seleccionadas teniendo en cuenta la información que fue suministrada en las entrevistas realizadas a los diferentes funcionarios del instituto.

El puntaje total de la estratificación se determinó por la suma de los rangos de valores escogidos en la tabla, en el caso del instituto este es igual a 21 puntos.

El nivel de estratificación del instituto de acuerdo con el puntaje anterior se define en relación a los rangos de valores de la siguiente tabla.

Tabla 24: Nivel estratificación del Instituto

PUNTOS	CLASIFICACIÓN
Menor a 11	BAJO
Entre 11 y 22	MEDIO
Mayor a 22	ALTO

Fuente: El autor

Conforme al puntaje de 21 puntos obtenido por el instituto, el nivel de estratificación de este se encuentra en MEDIO.

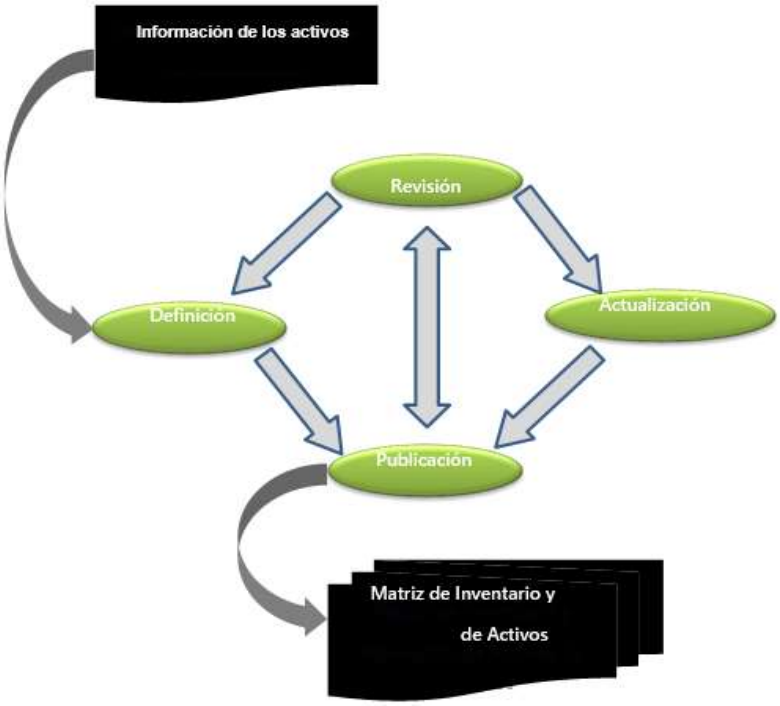
9. FASE 2. IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

La siguiente fase se desarrolla con base a las recomendaciones trazadas en la guía número 5 versión 1.0 del 15/03/2016 para la gestión y clasificación de activos de la información del modelo de seguridad y privacidad de la información impartida por el Ministerio de las Tecnologías de la Información y las comunicaciones MINTIC.

Para el desarrollo de este objetivo también se tuvieron en cuenta las recomendaciones de la Norma ISO 27005 del 2009, la ley 1712 del 2014 mediante la cual se creó la Ley de Trasparencia y del derecho de acceso a la información pública nacional.

La clasificación de activos de información debe realizarse en función de los requerimientos legales vigentes, el valor, la criticidad y susceptibilidad en la divulgación o no autorizada que se mencionan en las políticas del modelo de seguridad y privacidad de la información.

Figura 9: Clasificación de activos



Fuente:http://mintic.gov.co/gestionti/615/articles 5482_G5_Gestion_clasificacion.pdf

9.1 GUÍA PARA EL REGISTRO DE ACTIVOS DE INFORMACIÓN

9.1.1 Matriz de identificación, valoración y clasificación de activos de información

Es una matriz de consulta donde se encuentra consignada toda la información obtenida de las entrevistas realizadas a los líderes de proceso, aplicando las siguientes partes:

PARTE I - Identificación de Activos

Consiste en identificar toda la información necesaria de los activos en conjunto con el personal a cargo, para así determinar la valoración y el nivel de clasificación del activo, para ello se definen los siguientes criterios:

Tabla 25: Identificación de activos

I. IDENTIFICACIÓN DEL ACTIVO DE INFORMACIÓN							
ID	TIPO DE PROCESO	PROCESO	SUBPROCESO	SEDE	ACTIVO DE INFORMACIÓN	DESCRIPCIÓN DEL ACTIVO	IDIOMA

Fuente: NTC/ISO 27005:2009

ID: Número único consecutivo que identifica al activo dentro del inventario.

Tipo de Proceso: Clasificación del proceso en función de su finalidad.

Proceso: Nombre del proceso al cual pertenece el activo de información.

Subproceso: Nombre del subproceso al cual pertenece el activo de información.

Sede: Seccional en donde se encuentra ubicado el activo de información.

Activo de Información: Nombre del elemento de información que genere valor para el proceso y que debe protegerse. La información es un activo primario y no de soporte[13].

Descripción del activo: Explicación de las características más relevantes del activo identificado.

Idioma: Especifica si se encuentra en algún idioma especial o si se encuentra en español.

PARTE II – PROPIEDAD

Se define el propietario de la información y el custodio de la información, con el fin de determinar quiénes serán los responsables a la hora de brindar seguridad en caso de accesos no autorizados, modificaciones, o destrucción, donde se vean comprometidos los objetivos de seguridad de la información.

Tabla 26: Propiedad del Activo

II. PROPIEDAD DEL ACTIVO	
PROPIETARIO DE LA INFORMACIÓN	CUSTODÍO DE LA INFORMACIÓN

Fuente: Guía 5 - Gestión y Clasificación de Activos - MSPI

Propietario de la información: Es una parte designada del instituto, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento se clasifican adecuadamente, y de dar las directrices de uso del activo, autorizar privilegios, definir el ciclo de vida del mismo y revisar periódicamente las restricciones y

[13] NTC/ISO 27005:2009

clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso[14].

Custodio de la información[15]: Es una parte designada del instituto, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado.

PARTE III – SOPORTE DE LOS ACTIVOS DE INFORMACIÓN
Se identifica el lugar físico o lógico en donde se encuentra soportado el activo de información identificado.

Tabla 27: Soporte de los activos de información

III. SOPORTE DE LOS ACTIVOS DE INFORMACION																				
HARDWARE				SOFTWARE					REDES			SITIO					PERSONAL		PROCEDIMENTAL Y ESTRUCTURAL		DESCRIPCIÓN DE LA UBICACIÓN
Servidor	Computadora de Escritorio	Dispositivo Móvil	Medio extraíble	Aplicación	Ofimática	Base de datos	Sistema operativo	Correo electrónico	Red Pública	WAN Privada	LAN	Centro de Datos	Archivo central	Archivo de gestión	Oficinas Nacionales	Sitio externo	Personal Interno	Personal Externo	Políticas	Procedimientos	

Fuente: NTC/ISO 27005:2009

HARDWARE: Consta de todos los elementos físicos que dan soporte a los activos de información de manera digital[16].

[14] Guía 5 - Gestión y Clasificación de Activos - MSPI
[15] Guía 5 - Gestión y Clasificación de Activos - MSPI
[16] NTC/ISO 27005:2009

SOFTWARE: Se debe especificar si corresponde a un software de aplicación, software del sistema, herramientas de desarrollo y/o utilidades. El software se considera como un soporte a los activos de información[17].

REDES: Dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información.

SITIO: Comprende todos los lugares que contienen el activo de información o parte de éste, y los medios físicos que requieren para su funcionamiento.

PERSONAL: Consiste en todos los grupos de personas involucradas en la gestión, procesamiento, almacenamiento, control o custodia del activo de información.

PROCEDIMENTAL Y ESTRUCTURAL: políticas y procedimientos que son necesarios para que el instituto cumpla con los requisitos contractuales, legales o reglamentarios.

DESCRIPCIÓN DE LA UBICACIÓN: Hace referencia a la ubicación del activo sea física o digital de una forma más detallada.

PARTE IV – VALORACIÓN DEL ACTIVO

Luego de identificar los activos de información, el siguiente paso es valorarlos, es decir, se debe estimar qué valor tienen para el instituto y cuál es su importancia para la misma.

Tabla 28: Valoración de Activos

IV. VALORACIÓN ACTIVOS					
ATRIBUTOS DE LA (TRIADA)				TIPOS DE PROCESOS	
C	I	D	CID	PROCESO	VALOR DEL ACTIVO

Fuente: Guía 5 - Gestión y Clasificación de Activos – MSPI

[17] NTC/ISO 27005:2009

Para calcular el valor, se considera cuál puede ser el impacto que puede suponer para el instituto que un activo se vea afectado en relación a su disponibilidad, integridad y confidencialidad, para lo cual se establecen los siguientes atributos:

ATRIBUTOS DE LA TRIADA

Son criterios para darle la valoración del activo en términos de confidencialidad, integridad y disponibilidad de la información, es decir, qué tan importante es el activo para el proceso.

INTEGRIDAD: propiedad de salvaguardar la exactitud y estado completo de los activos de información.

Tabla 29: Valoración de Integridad

INTEGRIDAD		
VALOR	**NIVEL**	**CRITERIOS DE CLASIFICACIÓN**
5	MUY ALTO	La pérdida de exactitud y estado incompleto de la información, impacta negativamente tanto las finanzas y la reputación del instituto.
4	ALTO	La pérdida de exactitud y estado incompleto de la información, impacta negativamente la reputación del instituto.
3	MEDIO	La pérdida de exactitud y estado incompleto de la información, impacta negativamente las finanzas del instituto..
2	BAJO	La pérdida de exactitud y estado incompleto de la información, impacta negativamente a nivel operacional del instituto..
1	MUY BAJO	La pérdida de exactitud y estado incompleto de la información, no genera impacto alguno para del instituto..

Fuente: Guía 5 - Gestión y Clasificación de Activos – MSPI

CONFIDENCIALIDAD: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Tabla 30: Valoración de Confidencialidad

CONFIDENCIALIDAD		
VALOR	**NIVEL**	**CRITERIOS DE CLASIFICACIÓN**
5	MUY ALTO	Conocimiento y divulgación de la información Reservada, impacta negativamente tanto las finanzas y la reputación del instituto..
4	ALTO	Conocimiento y divulgación de la información Sensible, impacta negativamente la reputación del instituto..
3	MEDIO	Conocimiento y divulgación de la información Interna, impacta negativamente las finanzas del instituto..
2	BAJO	Conocimiento y divulgación de información Pública, impacta negativamente a nivel operacional del instituto.

Fuente: Guía 5 - Gestión y Clasificación de Activos – MSPI

9.2 TIPOLOGÍAS DE LOS ACTIVOS DE INFORMACIÓN

Tabla 31: Tipologías de los activos de información

COMPONENTES	TIPOLOGÍAS	DESCRIPCIÓN
Tipos de almacenamiento de activos de información	Digital	Todos los tipos de archivos en los diferentes formatos como por ejemplo: Bases de datos, fotos, audios, textos, videos. Etc.
	Físico	Toda la información en medio impresa como por ejemplo: Revistas, periódicos, carteleras, memorandos.

Ubicación y/o contenedores de activos de información	Hardware	Equipos complementarios de apoyo para las operaciones sobre algún activo de información.
	Almacenamiento Electrónico	Almacenamiento extraíble complementarios como USB, CD, DVD, discos duros externos, entre otros.
	Infraestructura Física	Instalaciones, redes, etc. para desarrollar una actividad específica, que ofrezca servicio requerido por IMN con el alojamiento de la información.
Responsables y custodios	Recurso Humano	Funcionario que realiza las funciones críticas para el Instituto, cuya ausencia desencadena el incumplimiento de las funciones.
Aplicaciones de procesamiento	Software	Todo sistema de información o programa requerido que requiera activos de información para cumplir tareas.

Fuente: El autor

9.3 IDENTIFICAR LOS ACTIVOS DE INFORMACIÓN

La identificación y clasificación de los activos de información es de mucha importancia debido a que se determina cuáles son los activos que posee el instituto y de qué manera son utilizados los roles y responsabilidades que tiene cada funcionario con los mismos, con este proceso también se reconoce el nivel de clasificación según su confidencialidad, integridad y disponibilidad de la información la cual debe tener a cada activo de información.

Con esta guía el líder o jefe del proceso debe solicitar la revisión por lo menos anualmente de la definición de los activos por parte del funcionario responsable del activo de información para validar si corresponde la idoneidad de este rol a dicho funcionario asignado por parte del instituto.

9.4 CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

La siguiente plantilla de clasificación permite identificar de forma estructurada y fácil los activos de información, con las siguientes pautas:

a.) Identificar de forma organizada los activos de información.

b.) Describir las características básicas de los activos de información.

c.) Clasificar los activos de información.

Tabla 32: Clasificación de los activos de información

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
PÚBLICA	BAJA	NO CRÍTICO.
USO INTERNO	MEDIA	MENOS CRÍTICO.
CONFIDENCIAL	ALTA	MISIÓN CRÍTICA.

Fuente: El autor

a.) La identificación se realiza de acuerdo a la respuesta con la cual se establecerá el nivel de sensibilidad.

CONFIDENCIALIDAD: El nivel de confidencialidad se determina cuando la respuesta es SI a cualquiera de las siguientes premisas.

Figura 10: Nivel de Confidencialidad

Publico	Es toda aquella información que el sujeto obligado genere, obtenga, posea, o sea administrada en su calidad.
	Es todo aquella información que actualmente este disponible al publico.
	Es toda aquella información utilizada para mercadeo publico en general.
	Es la información desplegada al publico sin beneficiar a la competencia, sin impactar de forma negativa al instituto, sin ninguna brecha de seguridad.
	Información disponible al publico por medio de los medios de comunicación.
	Se refiere a todos los datos personales publicados, clasificados como tal como documentos públicos según la legislación o constitución política (El estado civil es un dato publico entre otros).
Uso Interno	Es toda aquella información asociada con las políticas, procedimientos, estándares, organigramas, comunicados internos, directorio telefónicos institucional.
	Es todo aquella información que se puede divulgar por medio de boletines, memorando internos, o publicar en la intranet.
	Es información que puede ser divulgada sin ninguna restricción a los funcionarios, pudiéndose ser divulgar a los usuarios externos con aprobación.
	Son todos los datos personales sin naturaleza intima, la cual es reservada o privada cuyo interés es para los funcionarios del instituto.
Confidencial	Toda aquella información a la cual se le debe guardar reserva, secreto, discreción, sean datos de los usuarios, o que se relacionen con la situación propia del instituto.
	Información secreta que solo esta disponible y puede ser suministrada a usuarios, procesos, entidades autorizadas.
	Se trata de la información cobijada por los derechos constitucionales, intimidad o fundamentada en el principio de secreto profesional.
	Informes, reportes, o investigaciones acerca de: Fraudes ilícitos, mala
	Información que incorpora datos específicos de protocolos de seguridad, como la llave pública de cifrado, password o firmas criptográficas.
	Información con datos privados reservados la cual solo se dispone al titular.
	Es toda la información que de despliega de forma restringida derivada de la naturaleza de datos con disposiciones legales.

Fuente: El autor

INTEGRIDAD: El nivel de integridad se determina cuando la respuesta es SI a cualquiera de las siguientes premisas.

Figura 11: Nivel de Integridad

Bajo	La perdida o modificación no autorizada de los activos de información no implica en daños a la institución.
	La perdida o modificación no autorizada de los activos de información no causa sanciones o perdidas económicas para el instituto.
	La perdida o modificación no autorizada de los activos de información no causa mala reputación o imagen negativa para el instituto.
	La perdida o modificación no autorizada de los activos de información no genera reclamaciones por los usuarios o funcionarios del instituto.
	La perdida o modificación no autorizada de los activos de información no afecta la oportunidad de la información del instituto.
Medio	La perdida o modificación no autorizada de la Información causa multas, sanciones económicas recuperables para el instituto.
	La perdida o modificación no autorizada de la Información podrían causar un poco de mala imagen o perdida de la reputación para el instituto.
	La perdida o modificación no autorizada de la Información podrían generar reclamaciones por parte de los usuarios o proveedores para el instituto, sin
	La perdida o modificación no autorizada de una Información podrían generar perjuicios legales para el instituto.
	La perdida o modificación no autorizada de una Información podrían incurrir en reprocesos con aumento de carga operativa.
Alto	La perdida o modificación no autorizada de una Información puede generar sanciones económicas, multas por autoridades legales para el instituto.
	La perdida o modificación no autorizada de una Información puede generar sanciones económicas para el instituto.
	La perdida o modificación no autorizada de una Información puede hacer reclamaciones por los usuarios y/o proveedores.
	La perdida o modificación no autorizada de una Información puede generar inconvenientes judiciales.
	La perdida o modificación no autorizada de una Información repercute en perdida de información critica en el instituto o terceros sin poder recuperar.

Fuente: El autor

DISPONIBILIDAD: El nivel de disponibilidad se determina cuando la respuesta es SI a cualquiera de las siguientes premisas.

Figura 12: Nivel de disponibilidad

Bajo	La perdida o modificación no autorizada de los activos de información no implica en daños a la institución.
	La perdida o modificación no autorizada de los activos de información no causa sanciones o perdidas económicas para el instituto.
	La perdida o modificación no autorizada de los activos de información no causa mala reputación o imagen negativa para el instituto.
	La perdida o modificación no autorizada de los activos de información no genera reclamaciones por los usuarios o funcionarios del instituto.
	La perdida o modificación no autorizada de los activos de información no afecta la oportunidad de la información del instituto.
Medio	La perdida o modificación no autorizada de la Información causa multas, sanciones económicas recuperables para el instituto.
	La perdida o modificación no autorizada de la Información podrían causar un poco de mala imagen o perdida de la reputación para el instituto.
	La perdida o modificación no autorizada de la Información podrían generar reclamaciones por parte de los usuarios o proveedores para el instituto, sin
	La perdida o modificación no autorizada de una Información podrían generar perjuicios legales para el instituto.
	La perdida o modificación no autorizada de una Información podrían incurrir en reprocesos con aumento de carga operativa.
Alto	La perdida o modificación no autorizada de una Información puede generar sanciones económicas, multas por autoridades legales para el instituto.
	La perdida o modificación no autorizada de una Información puede generar sanciones económicas para el instituto.
	La perdida o modificación no autorizada de una Información puede hacer reclamaciones por los usuarios y/o proveedores.
	La perdida o modificación no autorizada de una Información puede generar inconvenientes judiciales.
	La perdida o modificación no autorizada de una Información repercute en perdida de información critica en el instituto o terceros sin poder recuperar.

Fuente: El autor

b.) Identificar y clasificar los activos de información con la tabla de retención documental del instituto.

Ver Anexo A.

C.) clasificación de los activos de información con base a los contenedores críticos.

Teniendo en cuenta la anterior clasificación de los activos, ahora se debe seleccionar los contenedores que tiene cada activo de información crítico para el instituto. Por lo tanto es importante confirmar si el activo de información cumple con las condiciones que se describen a continuación:

Figura 13: Clasificación criterios de contenedores

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CRISTICIDAD DEL CONTENEDOR
Confidencial	Alta	Misión Crítica	Alta
Confidencial	Alta	Menos Crítico	Alta
Confidencial	Alta	NO Critico	Alta
Confidencial	Media	Misión Crítica	Alta
Confidencial	Media	Menos Crítico	Media
Confidencial	Media	NO Critico	Media
Confidencial	Baja	Misión Crítica	Alta
Confidencial	Baja	Menos Crítico	Media
Confidencial	Baja	NO Critico	Media
Uso Interno	Alta	Misión Crítica	Alta
Uso Interno	Alta	Menos Crítico	Alta
Uso Interno	Alta	NO Critico	Media
Uso Interno	Media	Misión Crítica	Media
Uso Interno	Media	Menos Crítico	Media
Uso Interno	Media	NO Critico	Media
Uso Interno	Baja	Misión Crítica	Media
Uso Interno	Baja	NO Critico	Media
Uso Interno	Baja	Menos Crítico	Media
Público	Alta	NO Critico	Media
Público	Alta	Misión Crítica	Alta
Público	Alta	Menos Crítico	Media
Público	Media	NO Critico	Media
Público	Media	Misión Crítica	Bajo
Público	Media	Menos Crítico	Bajo
Público	Bajo	Misión Crítica	Media
Público	Bajo	Menos Crítico	Bajo
Público	Bajo	NO Critico	Bajo

Fuente: El autor

A Continuación se describen los activos explorados mediante la identificación de los procesos misionales de la oficina de las tecnologías de la información para el Instituto Museo Nacional IMN.

Figura 14: Listado de servidores

Nombre	Tipo de Servidor	Sistema Operativo	Versión Sistema Operativo	Direccionamiento IP	Funcionalidad	COMPATIBLE
Bog-dc-02	Virtual	Windows	Windows 2012 server R2	[redacted]	Controlador de dominio	SI
BOG-WEB-02	Virtual	Windows	Windows 2003 server	[redacted]	Servidor Web	SI
BOG-WEB-01	Virtual	Windows	Windows 2008 server	[redacted]	Servidor Web	SI
BOG-DC-01	Virtual	Windows	Windows 2012 server R2	[redacted]	Controlador de dominio	SI
APOLO	Fisico	Windows	Windows 2003 server	[redacted]	File Server	SI
Monitoreo Vmware	Virtual	Windows	Windows 2012 server R2	[redacted]	Gestion de Monitoreo	SI
BOG-HELP-02	Virtual	Windows	Windows 2008 server	[redacted]	Aplicaciones mesa de ayuda /Web/cliente servidor	SI
BOG-HELP-01	Virtual	Windows	Windows 2008 server	[redacted]	Aplicaciones mesa de ayuda /Web/cliente servidor	SI
MARTE	Fisico	Windows	Windows 2000 server	[redacted]	Aplicaciones facturacion/cliente servidor	SI
BOG-BOK-01	Fisico	Windows	Windows 2008 server	[redacted]	Aplicaciones dataprotector	SI
BOG-FENICA-01	Virtual	Windows	Windows 2008 server	[redacted]	Aplicaciones /cliente servidor	SI
BOG-WEB-05	Virtual	Windows	Windows 2008 server	[redacted]	Servidor Web	SI
ABACOX	Virtual	Windows	Windows 2008 server	[redacted]	Servidor Web	SI
BOG-BD-01	Virtual	Windows	Windows 2008 server	[redacted]	Servidor Base de Datos	SI
BOG-SIS-01	Virtual	Windows	Windows 2003 server	[redacted]	Servidor Web	SI
BOG-BD-06	Virtual	Windows	Windows 2008 server	[redacted]	Servidor Base de Datos	SI
BOG-EPO-02	Virtual	Windows	Windows 2012 server R2	[redacted]	Aplicación mcafee	SI
BOG-WEB-03T	Virtual	Windows	Windows 2008 server	[redacted]	Servidor Web	SI
BOG-WEB-06	Virtual	Windows	Windows 2008 server	[redacted]	Servidor Web	SI
BOG-WEB-12	Virtual	Windows	Windows 2012 server R2	[redacted]	Servidor Web	SI
BOG-WEB-15	Virtual	Windows	Windows 2008 server	[redacted]	Servidor Web	SI
BOG-WEB-14	Virtual	Windows	Windows 2008 server	[redacted]	Servidor Web	SI
BOG-EPO-1	Virtual	Windows	Windows 2012 server R2	[redacted]	Servidor Web	SI
BOG-VCENTER-1	Virtual	Windows	Windows 2012 server R2	[redacted]	Aplicación Vmware	SI
BOG-WEB-16	Virtual	Windows	Windows 2008 server	[redacted]	Servidor Web	SI
BOG-WEB-17	Virtual	Windows	Windows 2008 server	[redacted]	Servidor Web	SI
BOG-SYNC-01	Virtual	Windows	Windows 2012 server R2	[redacted]	Aplicación Office 365	SI
BOG-HYB-01	Virtual	Windows	Windows 2012 server R2	[redacted]	Aplicación Office 365	SI
BOG-IMPR-01	Virtual	Windows	Windows 2012 server R2	[redacted]	Aplicación de Impresión	SI
bog-bd-01-sf	Virtual	Windows	Windows 2008 server	[redacted]	Servidor Base de Datos	SI
bog-web3 (SISPAP y SNR)	Virtual	Windows	Windows 2008 server	[redacted]	Servidor Web	SI
MADR-WEB-01	Virtual	Windows	Windows 2012 server R2	[redacted]	Servidor Web	SI
MADR-APP-01	Virtual	Windows	Windows 2012 server R2	[redacted]	Servidor Web	SI
MADR-BD-01	Virtual	Windows	Windows 2012 server R2	[redacted]	Servidor Base de Datos	SI
BOG-BD-1	Virtual	Windows	Windows 2012 server R2	[redacted]	Servidor Base de Datos	SI
BOG-WEB-02	Virtual	Windows	Windows 2003 server	[redacted]	Servidor Web	SI
BOG-DES-01	Virtual	Windows	Windows 2012 server R2	[redacted]	Servidor Web	SI
BOG-WEB-09	Fisico	Windows	Windows 2008 server	[redacted]	Servidor Web	SI
BOG-WEB-08	Fisico	Windows	Windows 2008 server	[redacted]	Servidor Web	SI
BOG-WEB-10	Fisico	Windows	Windows 2008 server	[redacted]	Servidor Web	SI
BOG-WEB-11	Fisico	Windows	Windows 2008 server	[redacted]	Servidor Web	SI
BOG-FAX-01	Fisico	Windows	Windows 2008 server	[redacted]	Servidor Web	SI
BOG-BOK-02	Fisico	Windows	Windows 2008 server	[redacted]	Aplicación Backup usuario final	SI
Atlantico-dc-01	Fisico	Windows	Windows 2008 server	[redacted]	Controlador de dominio secundario	SI
Bucaramanga-dc-01	Fisico	Windows	Windows 2008 server	[redacted]	Controlador de dominio secundario	SI
Caldas-dc-01	Fisico	Windows	Windows 2008 server	[redacted]	Controlador de dominio secundario	SI
Cali-dc-01	Fisico	Windows	Windows 2008 server	[redacted]	Controlador de dominio secundario	SI
Caqueta-dc-01	Fisico	Windows	Windows 2008 server	[redacted]	Controlador de dominio secundario	SI
Cesar-dc-01	Fisico	Windows	Windows 2008 server	[redacted]	Controlador de dominio secundario	SI
Cordoba-dc-01	Fisico	Windows	Windows 2008 server	[redacted]	Controlador de dominio secundario	SI
Cucuta-dc-01	Fisico	Windows	Windows 2008 server	[redacted]	Controlador de dominio secundario	SI
Guajira-dc-01	Fisico	Windows	Windows 2008 server	[redacted]	Controlador de dominio secundario	SI
Huila-dc-01	Fisico	Windows	Windows 2008 server	[redacted]	Controlador de dominio secundario	SI
Ibague-dc-01	Fisico	Windows	Windows 2008 server	[redacted]	Controlador de dominio secundario	SI
Ind-dc-01	Fisico	Windows	Windows 2008 server	[redacted]	Controlador de dominio secundario	SI
Sucre-dc-01	Fisico	Windows	Windows 2008 server	[redacted]	Controlador de dominio secundario	SI
Pereira-dc-01	Fisico	Windows	Windows 2008 server	[redacted]	Controlador de dominio secundario	SI
Node1	Fisico	linux	Linux redhat 6.5	[redacted]	Cluster Nodo 1 (oracle)	SI
Node2	Fisico	linux	Linux redhat 6.5	[redacted]	Cluster Nodo 2 (oracle)	SI
Bog-db-02	Virtual	linux	Linux redhat 6.5	[redacted]	Servidor de base de datos (oracle)	SI
Bog-web04	Virtual	linux	Linux debian 6	[redacted]	Servidor de Aplicaciones (SIGMA)	SI
Bog-db-05	Virtual	linux	Linux Oracle	[redacted]	Servidor de Base de datos Pruebas (oracle)	SI
Bog-web04	Virtual	linux	Linux debian 8	[redacted]	Servidor de Aplicaciones (Sisifo, Siscop)	SI
Bog-web07	Virtual	linux	Linux debian 8	[redacted]	Servidor de Aplicaciones Pruebas (Sigma, sisifo, siscop)	SI
Bog-db-03	Virtual	linux	Linux debian 8	[redacted]	Servidor de Base de datos Maria DB	SI
Bog-icanuke-01	Fisico	linux	Linux debian 8	[redacted]	Servidor de Base de aplicaciones icanuke	SI
Bog-dspace	Virtual	linux	Linux debian 8	[redacted]	Servidor de Base de aplicaciones sipci - dspace	SI

Fuente: Instituto Museo Nacional

Figura 15: Listado de equipos de comunicaciones

Item	Equipo	Marca	Modelo	Sistema Operativo	Rol
1	Switch	Cisco	WS-C3750G-48PS-S	12.2(35)SE5	
2	Switch	Avaya			
3	Switch	Cisco	WS-C3750G-48PS-S	12.2(35)SE5	
4	Switch	Cisco	WS-C2960-24TC-L	12.2(44)SE6	
5	Switch	Cisco	WS-C3750G-48PS	12.2(35)SE5	
6	Switch	Cisco	WS-C3750G-48PS	12.2(35)SE5	
7	Switch	Cisco	WS-C3750G-48PS	12.2(35)SE5	
8	Switch	Avaya			
9	Switch	Cisco	WS-C3750X-48	12.2(55)SE3	
10	Switch	HP	A5120-48G-PoE+	5.20.99	
11	Switch	Cisco	WS-C3750G-12S	12.2(35)SE5	
12	Switch	HP	A5120-48G-PoE+	5.20.99	
13	Switch	Cisco	WS-C2960S-24PS-L	12.2(53)SE2	
14	Switch	Cisco	WS-C2960-24TC-L	12.2(50)SE4	
15	Switch	Cisco	WS-C2960-24TC-L	12.2(50)SE4	
16	Switch	Cisco	WS-C2960-24TC-L	12.2(50)SE4	
17	Switch	Cisco	WS-C2960-24TC-L	12.2(50)SE4	
18	Switch	Cisco	WS-C3750G-24PS	12.2(35)SE5	
19	Switch	Cisco	WS-C3750G-24PS	12.2(35)SE5	
20	Switch	Cisco	WS-C3750G-24PS	12.2(35)SE5	
21	Switch	Cisco	WS-C3750G-24PS	12.2(35)SE5	
22	Switch	Cisco	WS-C3750G-24PS	12.2(35)SE5	
23	Switch	HP	A5120-48G-PoE+	5.20	
24	Switch	HP	A5120-24G-PoE+	5.20	
25	Switch	HP	A5120-48G-PoE+	5.20	
26	Switch	HP	A5120-24G EI	5.20	
27	Switch	HP	A5120-48G-PoE+	5.20	
28	Switch	HP	A5120-24G-PoE+	5.20	
29	Switch	HP	A5500-24G-4SFP	5.20.99	
30	Switch	HP	A5120-48G-PoE+	5.20	
31	Switch	HP	A5120-24G-PoE+	5.20	
32	Switch	HP			
33	Switch	Cisco	WS-C3560X-48	12.2(55)SE3	
34	Switch	Cisco	WS-C2960-24TC-L	12.2(50)SE5	
35	Switch	Cisco	WS-C2960-24TC-L	12.2(50)SE4	
36	Switch	Avaya	P330	3.0.5	
37	AP	HP	MSM 460	6.5.2.0-22155	
38	AP	HP	MSM 460	6.5.2.0-22155	
39	AP	HP	MSM 460	6.5.2.0-22155	
40	AP	HP	MSM 460	6.5.2.0-22155	
41	AP	HP	MSM 460	6.5.2.0-22155	
42	AP	HP	MSM 460	6.5.2.0-22155	
43	AP	HP	MSM 460	6.5.2.0-22155	
44	AP	HP	MSM 460	6.5.2.0-22155	
45	AP	HP	MSM 460	6.5.2.0-22155	

Figura 15 (Continuación)

Item	Equipo	Marca	Modelo	Sistema Operativo	Rol
46	AP	HP	MSM 460	6.5.2.0-22155	
47	AP	HP	MSM 460	6.5.2.0-22155	
48	AP	HP	MSM 460	6.5.2.0-22155	
49	AP	HP	MSM 460	6.5.2.0-22155	
50	AP	HP	MSM 460	6.5.2.0-22155	
51	AP	HP	MSM 460	6.5.2.0-22155	
52	AP	HP	MSM 460	6.5.2.0-22155	
53	Controladora	HP	MSM 720	6.5.2.0-22155	
54	Planta Telefonica	Cisco	C3845-IPVOICEK9-M	12.4(20)T5	
55	Planta Telefonica	Cisco	C3825-SPSERVICESK9-M	12.4(22)T4	
56	Voz Analoga	Cisco	VG224	12.4(13r)T7	
57	Voz Analoga	Cisco	VG224	12.4(22)T3	
58	Voz Analoga	Cisco	VG224	12.4(22)T3	
59	Voz Analoga	Cisco	VG224	12.4(22)T3	
60	Planta Telefonica	Panasonic	TDE 100	N/A	
61	Planta Telefonica	Panasonic	TDE 100	N/A	
62	Planta Telefonica	Panasonic	NCP500	N/A	
63	Planta Telefonica	Panasonic	NCP500	N/A	
64	Planta Telefonica	Panasonic	TDE 100	N/A	
65	Planta Telefonica	Panasonic	TDE 100	N/A	
66	Planta Telefonica	Panasonic	TDE 100	N/A	
67	Planta Telefonica	Panasonic	TDE 100	N/A	
68	Planta Telefonica	Panasonic	TDE 100	N/A	
69	Planta Telefonica	Panasonic	TDE 100	N/A	
70	Planta Telefonica	Panasonic	TDE 100	N/A	
71	Planta Telefonica	Panasonic	TDE 100	N/A	
72	Planta Telefonica	Panasonic	TDE 100	N/A	
73	Planta Telefonica	Panasonic	TDE 100	N/A	
74	Planta Telefonica	Panasonic	NCP500	N/A	
75	Planta Telefonica	Panasonic	TDE 100	N/A	
76	Planta Telefonica	Panasonic	TDE 100	N/A	
77	Planta Telefonica	Panasonic	TDA 100	N/A	
78	Planta Telefonica	Panasonic	NCP500	N/A	
79	Planta Telefonica	Panasonic	NCP500	N/A	
80	Planta Telefonica	Panasonic	TDE 100	N/A	
81	Planta Telefonica	Panasonic	TDE 100	N/A	
82	Planta Telefonica	Panasonic	TDE 100	N/A	
83	Planta Telefonica	Panasonic	TDE 100	N/A	
84	Planta Telefonica	Panasonic	NCP1000	N/A	
85	Telefono	Cisco	7940	N/A	
86	Telefono	Cisco	7942	N/A	
87	Telefono	Cisco	7911	N/A	
88	Telefono	Cisco	7962	N/A	
89	Telefono	Cisco	7975	N/A	
90	Telefono	Panasonic	NT366	N/A	

Figura 15 (Continuación)

Item	Equipo	Marca	Modelo	Sistema Operativo	Rol
91	Telefono	Panasonic	NT346	N/A	
92	Firewall	Checkpoint	SG 4800	Gaia R77.20	
93	Videoconferencia	Polycom	QDX-6000	Release 4.0.1-3040	
94	Videoconferencia	Polycom	QDX-6000	Release 4.0.1-3040	
95	Videoconferencia	Polycom	QDX-6000	Release 4.0.1-3040	
96	Videoconferencia	Polycom	QDX-6000	Release 4.0.1-3040	
97	Videoconferencia	Polycom	QDX-6000	Release 4.0.1-3040	
98	Videoconferencia	Polycom	QDX-6000	Release 4.0.1-3040	
99	Videoconferencia	Polycom	QDX-6000	Release 4.0.1-3040	
100	Videoconferencia	Polycom	QDX-6000	Release 4.0.1-3040	
101	Videoconferencia	Polycom	QDX-6000	Release 4.0.1-3040	
102	Videoconferencia	Polycom	QDX-6000	Release 4.0.1-3040	
103	Videoconferencia	Polycom	QDX-6000	Release 4.0.1-3040	
104	Videoconferencia	Polycom	QDX-6000	Release 4.0.1-3040	
105	Videoconferencia	Polycom	QDX-6000	Release 4.0.1-3040	
106	Videoconferencia	Polycom	QDX-6000	Release 4.0.1-3040	
107	Videoconferencia	Polycom	QDX-6000	Release 4.0.1-3040	
108	Videoconferencia	Polycom	QDX-6000	Release 4.0.1-3040	
109	Videoconferencia	Polycom	QDX-6000	Release 4.0.1-3040	
110	Videoconferencia	Polycom	QDX-6000	Release 4.0.1-3040	
111	Videoconferencia	Aethra	X5 y X3	Vega X5 Series 3 12.1.10	
112	Videoconferencia	Aethra	X5 y X3	Vega X5 Series 3 12.1.10	
114	D2DBackup System	HP	D2D4112	N/A	
115	Packet Shaper	HP	7500	N/A	
116	Enrutador Inalambrico	Trendnet	Trednet TEW-452brp	N/A	
117	Enrutador Inalambrico	Trendnet	Trednet TEW-452brp	N/A	
118	Enrutador Inalambrico	Trendnet	Trednet TEW-452brp	N/A	
119	Enrutador Inalambrico	Trendnet	Trednet TEW-452brp	N/A	
120	Enrutador Inalambrico	Trendnet	Trendnet tew-450apb	N/A	
121	Enrutador Inalambrico	Encore	ENHWI-2AN3	N/A	
122	Enrutador Inalambrico	Dlink	DLINK DI524	N/A	
123	Access Point	Tp-Link	TL-WA901ND	N/A	
124	Enrutador Inalambrico	LinkSys	WRT300N-V1	N/A	
125	Enrutador Inalambrico	Trendnet	TEW-452BRP	N/A	
126	Access Point	Tp-Link	WR741	N/A	
127	Enrutador Inalambrico	D-Link	DIR-610	N/A	
128	Access Point	Tp-Link	TL-WA801ND	N/A	
129	Access Point	Tp-Link	TL-WA901ND	N/A	
130	Enrutador Inalambrico	LinkSys	WAP4400N	N/A	
131	Enrutador Inalambrico	LinkSys	Cisco WRT320N	N/A	
132	Access Point	Tp-Link	TL-WA901ND	N/A	
133	Access Point	Tp-Link	TL-WA901ND	N/A	
134	Access Point	Tp-Link	TL-WR740N	N/A	
135	Access Point	Tp-Link	TL-WR841N	N/A	
136	Access Point	Tp-Link	TL-WR740N	N/A	
137	Access Point	Cisco	WAP321	N/A	
138	Access Point	linksys	Cisco wrt120n	N/A	
139	Access Point	Tp-Link	TL-WR841N	N/A	
140	Access Point	Tp-Link	TL-WR841N	N/A	
141	Access Point	Tp-Link	TL-WR741ND	N/A	
142	Access Point	Kozumi	K-1500NR	N/A	
143	Access Point	Kozumi	K-1500NR	N/A	
144	Access Point	3bumen		N/A	

Fuente: Instituto Museo Nacional

10. FASE 3. INFORME DE EVALUACIÓN DE RIESGOS DE SEGURIDAD

La evaluación de riesgos realizado en IMN contempló el proceso misional: Gestión de Información y Tecnologías descrito en el alcance.

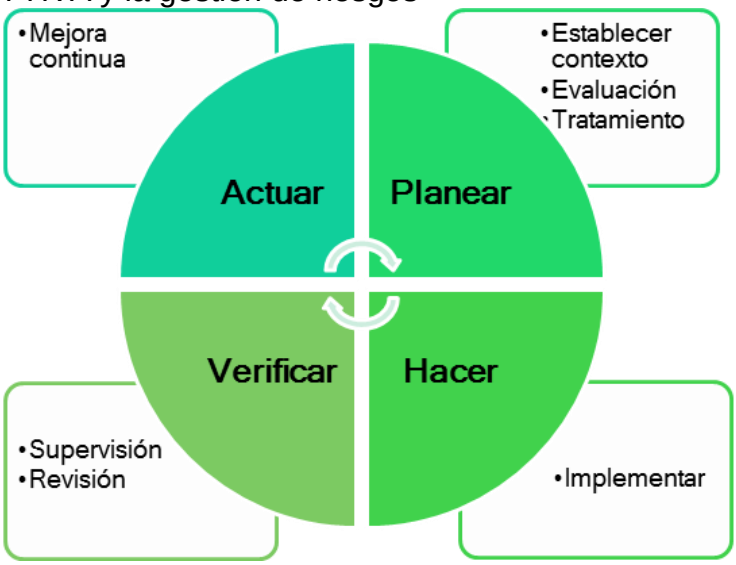
La técnica de análisis de riesgo para activos de información nos permite desde un punto de vista orientado al negocio o sistema y sistémico en su naturaleza, comprender claramente los riesgos sobre los activos de información a los que puede estar expuesto el instituto. Es recomendable contar con técnicas tradicionales para identificar los riesgos específicos asociados a los activos y complementar este proceso en la medida de lo posible con la identificación de puntos críticos de fallas, análisis de disponibilidad, análisis de vulnerabilidad, análisis de confiabilidad y árboles de falla. La metodología propuesta en este documento comprende, como se detallará más adelante, las siguientes actividades principales: establecimiento del contexto, identificación riesgos, estimación de riesgos, evaluación de riesgos, tratamiento de riesgo y aceptación del riesgo según lo propuesto por ISO 31000 e ISO 27005:

Figura 16: Estructura general de la metodología de riesgos

Fuente: El Autor.

La gestión del riesgo dentro de la seguridad de la información se puede también enmarcar dentro del ciclo de planear, hacer, verificar y actuar (PHVA) tal como se muestra en la siguiente ilustración (ISO 27001:2013):

Figura 17: Ciclo PHVA y la gestión de riesgos

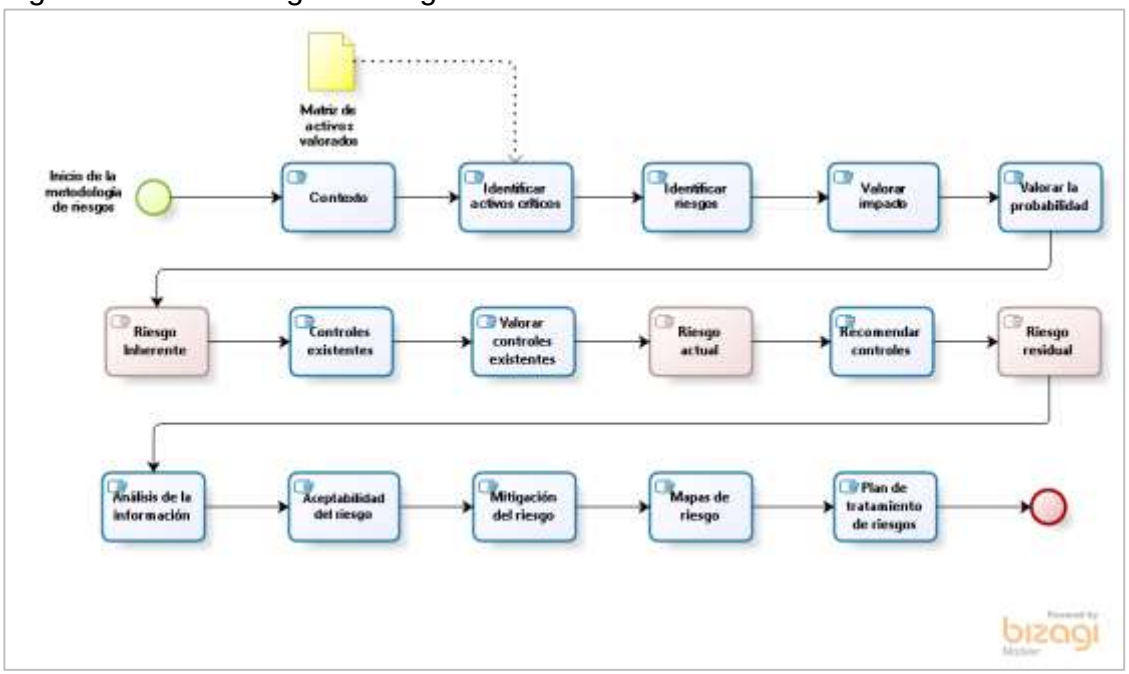


Fuente: El Autor.

10.1 METODOLOGIA UTILIZADA EN LA EVALUACION DE RIESGO.

En la siguiente figura se puede observar las fases propuestas para la metodología de análisis de riesgos para los activos de información del IMN. Esta metodología parte del contexto del instituto. y de los procesos (misionales y de apoyo) definidos con el fin de focalizar en ellos los riesgos identificados en el IMN La metodología fue implementada en la Matriz de Riesgos del IMN y en este documento Informe de Evaluación de Riesgos se presentarán los resultados obtenidos luego de la realización de este proceso con explicaciones adicionales sobre los hallazgos.

Figura 18: Metodología de riegos

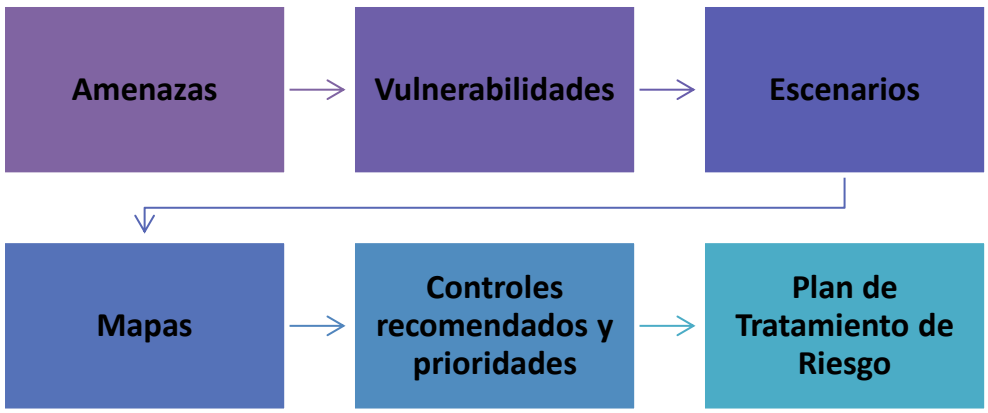


Fuente: El Autor.

10.2 INFORME DE RESULTADOS

A continuación presentamos la figura que representa la estructura con que se presentarán los resultados obtenidos luego del análisis de riesgos:

Figura 19: Estructura del informe



Fuente: El Autor.

10.3 INFORME DE VULNERABILIDADES

Las vulnerabilidades son debilidades de un activo y que pueden ser explotadas por una o más amenazas, afectando, ya sea la disponibilidad, la integridad o la confidencialidad. A continuación usando vulnerabilidades típicas y las extraídas de las entrevistas realizadas en el IMN, se presenta el listado de vulnerabilidades, el tipo de soporte y número de activos afectados, y para cada una de ellas se estima una criticidad cualitativa y una cuantitativa:

Tabla 33: Informe de Vulnerabilidades

Tipo de Soporte	Subtipo de Soporte	Número de activos Alto y Muy Alto	Vulnerabilidades	Criticidad cualitativa	Criticidad cuantitativa
HARDWARE	Servidor	23	Ausencia de servidor centralizado de archivos seguro	3	2
	Computador de escritorio	45	Ausencia de respaldo para archivos en PC	5	3
	Computador de escritorio	45	Uso incorrecto de hardware	3	3
	Computador de escritorio	45	No respaldo de información digital importante	5	3
	Dispositivo Móvil	3	Uso de portátiles sin la protección adecuada fuera de las instalaciones	5	1
	Dispositivo Móvil	3	Configuración insegura de dispositivos móviles	5	1
	Dispositivo Móvil	3	Uso de dispositivos móviles inseguros en el trabajo	4	1
	Medio extraíble	1	Uso de USB sin la protección adecuada	5	1
SOFTWARE	Aplicación	14	No se cuenta con un sistema de Logs (registro) centralizado	3	1
	Aplicación	14	Uso incorrecto de software	3	1
	Aplicación	14	Ausencia de procedimientos formales y usados para el desarrollo seguro	3	1
	Aplicación	14	Ausencia de estándares de configuración	2	1
	Ofimática	9	No respaldo de información digital importante	5	1
	Base de datos	15	Ausencia de estándares de configuración en la Base de datos	4	1

Tipo de Soporte	Subtipo de Soporte	Número de activos Alto y Muy Alto	Vulnerabilidades	Criticidad cualitativa	Criticidad cuantitativa
	Base de datos	15	Configuración insegura de la Base de datos	5	1
	Sistema operativo	19	No se realiza endurecimiento del sistema operativo	4	2
	E-MAIL	31	Ausencia de buenas prácticas de seguridad para el uso del correo	3	2
REDES	Red Pública	40	Uso inseguro de tecnologías de almacenamiento en la nube	2	3
	WAN Privada	14	Ausencia de supervisión de la red WAN privada	2	1
	LAN	14	No se realiza gestión de la capacidad en la red	2	1
	LAN	14	No se realiza gestión de la disponibilidad en la red	2	1
	LAN	14	No registro de logs de los dispositivos de red	3	1
SITIO	Datacenter	23	Ubicación no segura del Datacenter	5	2
	Datacenter	23	Ausencia de control formal sobre condiciones ambientales en Datacenter	3	2
	Datacenter	23	Presencia de material inflamable en el Datacenter	3	2
	Datacenter	23	Ausencia de planta generadora alterna	3	2
	Archivo central	5	No aplica		
	Archivo de gestión	61	Ubicación no segura del archivo físico	4	4
	Archivo de gestión	61	Ausencia de control formal sobre condiciones ambientales en archivo	3	4
	Archivo de gestión	61	No respaldo de información física importante	5	4
	Archivo de gestión	61	Localizaciones expuestas a inundaciones	4	4
	Oficinas Nacionales	85	No se escolta personal externo o visitantes	5	5
	Sitio externo	7	No aplica		
PERSONAL	Personal Interno	86	Falta de sensibilización en seguridad de la información	5	5
	Personal Interno	86	Escritorio no limpio	5	5
	Personal Interno	86	Insuficientes controles de acceso y de ubicación de la sede principal	5	5

Tipo de Soporte	Subtipo de Soporte	Número de activos Alto y Muy Alto	Vulnerabilidades	Criticidad cualitativa	Criticidad cuantitativa
	Personal Interno	86	Ausencia de sensibilización en el uso correcto de los procedimientos	5	5
	Personal Interno	86	Insuficiente entrenamiento para la creación de contraseñas	5	5
	Personal Externo	0	Falta de sensibilización en seguridad de la información	5	1
PROCEDIMENTAL Y ESTRUCTURAL	Políticas	1	Ausencia de políticas para el uso de criptografía	4	1
	Políticas	1	Ausencia de políticas para el borrado seguro y eliminación de equipos	3	1
	Políticas	1	No se realiza revisión de documentos de seguridad de la información	3	1
	Políticas	1	Ausencia de manual para asignar roles y responsabilidades	4	1
	Políticas	1	Política para el uso de controles criptográficos	4	1
	Procedimientos	1	Ausencia de estándares de configuración para TI	4	1
	Procedimientos	1	Ausencia de procedimientos para TI	4	1
	Procedimientos	1	No se cuenta con políticas y procedimientos de desarrollo seguro	4	1
	Procedimientos	1	No se cuenta con un plan de continuidad del negocio	5	1
	Procedimientos	1	Ausencia de auditorías formales y regulares	3	1
	Procedimientos	1	Falta de procedimientos formales para el análisis de vulnerabilidades	4	1
	Procedimientos	1	Falta de políticas y procedimientos para el uso de dispositivos móviles	4	1
	Procedimientos	1	Ausencia de procedimientos para la gestión de incidentes de seguridad	5	1
	Procedimientos	1	Ausencia de políticas y procedimientos para la gestión del cambio	5	1
	Procedimientos	1	Ausencia de políticas y procedimientos para la transferencia de información	5	1
	Procedimientos	1	Ausencia de políticas y procedimientos para los datos de prueba	3	1

Tipo de Soporte	Subtipo de Soporte	Número de activos Alto y Muy Alto	Vulnerabilidades	Criticidad cualitativa	Criticidad cuantitativa
	Procedimientos	1	Ausencia de políticas y procedimientos para el uso de dispositivo personales	5	1
	Procedimientos	1	Ausencia de políticas y procedimientos para el trabajo remoto	3	1
	Procedimientos	1	Ausencia de políticas y procedimientos para el cifrado del disco duro de PC´s	4	1
	Procedimientos	1	Ausencia de políticas y procedimientos para acceso móvil al correo electrónico	5	1
	Procedimientos	1	No se realiza revisión de documentos de seguridad de la información	3	1

Fuente: El Autor.

A continuación se presentan las vulnerabilidades con mayor impacto:

Tabla 34: Vulnerabilidades con mayor impacto

Vulnerabilidades	Criticidad cualitativa	Criticidad cuantitativa	Total
No se escolta personal externo o visitantes	5	5	10
Falta de sensibilización en seguridad de la información	5	5	10
Escritorio no limpio	5	5	10
Insuficientes controles de acceso y de ubicación de la sede principal	5	5	10
Ausencia de sensibilización en el uso correcto de los procedimientos	5	5	10
Insuficiente entrenamiento para la creación de contraseñas	5	5	10

Fuente: El Autor.

10.4 INFORME DE AMENAZAS

Las amenazas son las causas potenciales de un incidente no deseado, que puede provocar daños a un sistema o a la organización afectando en los activos de información ya sea la confidencialidad, la integridad o la disponibilidad. A continuación usando amenazas típicas y las extraídas de las entrevistas realizadas en el IMN se presenta el listado de amenazas, el tipo de soporte y número de activos afectados, y para cada una de ellas se estima una criticidad cualitativa y una cuantitativa:

Tabla 35: Informe de Amenazas

Tipo de Soporte	Subtipo de Soporte	Número de activos Alto y Muy Alto	Amenazas	Criticidad cualitativa	Criticidad cuantitativa
HARDWARE	Servidor	23	Pérdida de información	4	2
HARDWARE	Computador de escritorio	45	Pérdida de información	4	3
HARDWARE	Computador de escritorio	45	Indisponibilidad del PC´s	3	3
HARDWARE	Computador de escritorio	45	Pérdida de información	4	3
HARDWARE	Dispositivo Móvil	3	Robo de equipos	5	1
HARDWARE	Dispositivo Móvil	3	Virus	5	1
HARDWARE	Dispositivo Móvil	3	Virus	4	1
HARDWARE	Medio extraíble	1	Robo de medios	3	1
SOFTWARE	Aplicación	14	Pérdida de información	4	1
SOFTWARE	Aplicación	14	Abuso de derechos	4	1
SOFTWARE	Aplicación	14	Divulgación de la información	5	1
SOFTWARE	Aplicación	14	Falla de la aplicaciones críticas	4	1
SOFTWARE	Ofimática	9	Virus	4	1
SOFTWARE	Base de datos	15	Indisponibilidad de la base de datos	5	1
SOFTWARE	Base de datos	15	Modificación de la información	5	1
SOFTWARE	Sistema operativo	19	Robo de información	5	2
SOFTWARE	E-MAIL	31	Divulgación de la información	4	2
REDES	Red Pública	40	Robo de información	5	3
REDES	WAN Privada	14	Indisponibilidad de la red	3	1
REDES	LAN	14	Indisponibilidad de la red	3	1
REDES	LAN	14	Indisponibilidad de la red	3	1
REDES	LAN	14	Indisponibilidad de la red	3	1
SITIO	Datacenter	23	Destrucción de equipos	3	2

Tipo de Soporte	Subtipo de Soporte	Número de activos Alto y Muy Alto	Amenazas	Criticidad cualitativa	Criticidad cuantitativa
SITIO	Datacenter	23	Pérdida de servicios esenciales	5	2
SITIO	Datacenter	23	Destrucción de equipos	5	2
SITIO	Datacenter	23	Falla de potencia	3	2
SITIO	Archivo central	5	No aplica		
SITIO	Archivo de gestión	61	Daño físico en documentos	3	4
SITIO	Archivo de gestión	61	Daño físico en documentos	3	4
SITIO	Archivo de gestión	61	Pérdida de información	4	4
SITIO	Archivo de gestión	61	Daño físico en infraestructura	3	4
SITIO	Oficinas Nacionales	85	Robo de información	5	5
SITIO	Sitio externo	7	No aplica		
PERSONAL	Personal Interno	86	Procesamiento ilegal de información	5	5
PERSONAL	Personal Interno	86	Uso no autorizado de equipos	5	5
PERSONAL	Personal Interno	86	Ausencia de personal	5	5
PERSONAL	Personal Interno	86	Fallas en la operación	5	5
PERSONAL	Personal Interno	86	Robo de información	5	5
PERSONAL	Personal Externo	0	Robo de información	5	1
PROCEDIMENTAL Y ESTRUCTURAL	Políticas	1	Modificación de la información	5	1
PROCEDIMENTAL Y ESTRUCTURAL	Políticas	1	Copia fraudulenta de información	5	1
PROCEDIMENTAL Y ESTRUCTURAL	Políticas	1	Divulgación de la información	4	1
PROCEDIMENTAL Y ESTRUCTURAL	Políticas	1	Divulgación de la información	4	1
PROCEDIMENTAL Y ESTRUCTURAL	Políticas	1	Divulgación de la información	4	1
PROCEDIMENTAL Y ESTRUCTURAL	Procedimientos	1	Robo de información	5	1
PROCEDIMENTAL Y ESTRUCTURAL	Procedimientos	1	Indisponibilidad de TI	4	1
PROCEDIMENTAL Y ESTRUCTURAL	Procedimientos	1	Pérdida de información	4	1
PROCEDIMENTAL Y ESTRUCTURAL	Procedimientos	1	Indisponibilidad general de la sede	5	1
PROCEDIMENTAL Y ESTRUCTURAL	Procedimientos	1	Abuso de derechos	4	1
PROCEDIMENTAL Y ESTRUCTURAL	Procedimientos	1	Robo de información	5	1

Tipo de Soporte	Subtipo de Soporte	Número de activos Alto y Muy Alto	Amenazas	Criticidad cualitativa	Criticidad cuantitativa
PROCEDIMENTAL Y ESTRUCTURAL	Procedimientos	1	Escucha fraudulenta	4	1
PROCEDIMENTAL Y ESTRUCTURAL	Procedimientos	1	Pérdida de información	4	1
PROCEDIMENTAL Y ESTRUCTURAL	Procedimientos	1	Error en uso	3	1
PROCEDIMENTAL Y ESTRUCTURAL	Procedimientos	1	Escucha fraudulenta	5	1
PROCEDIMENTAL Y ESTRUCTURAL	Procedimientos	1	Copia fraudulenta de información	5	1
PROCEDIMENTAL Y ESTRUCTURAL	Procedimientos	1	Robo de información	5	1
PROCEDIMENTAL Y ESTRUCTURAL	Procedimientos	1	Pérdida de información	4	1
PROCEDIMENTAL Y ESTRUCTURAL	Procedimientos	1	Divulgación de la información	5	1
PROCEDIMENTAL Y ESTRUCTURAL	Procedimientos	1	Divulgación de la información	5	1
PROCEDIMENTAL Y ESTRUCTURAL	Procedimientos	1	Divulgación de la información	5	1

Fuente: El Autor.

A continuación se presentan las amenazas con mayor impacto:

Tabla 36: Amenazas con mayor impacto

Amenazas	Criticidad cualitativa	Criticidad cuantitativa
Robo de información	5	5
Procesamiento ilegal de información	5	5
Uso no autorizado de equipos	5	5
Ausencia de personal	5	5
Fallas en la operación	5	5

Fuente: El Autor.

10.5 INFORME DE ESCENARIOS DE RIESGOS

Teniendo en cuenta las vulnerabilidades sobre los activos, se procede a identificar amenazas asociadas a estas vulnerabilidades. Teniendo en cuenta los activos afectados y la valoración cuantitativa de estos riesgos, se diseñan los escenarios de riesgos, los que son clasificados según el tipo de riesgo (operativo, estratégico, financiero o legal), su origen (externo o interno) y finalmente el factor de riesgo (procesos, humanos, tecnología, infraestructura o externo).

A continuación se presenta la tabla con todos los escenarios de riesgo definidos para el IMN:

Tabla 37: Informe de escenarios de riesgo

ID	Escenarios de Riesgos	VALORACIÓN DEL ESCENARIO DEL RIESGO						
		Multas	Pérdida de credibilidad	Afectación operativa	Pérdida financiera	Pérdida de Información	VALORACION	Promedio de No. De Activos y valoración
1	Robo de información	3	5	3	5	5	21	54
2	Procesamiento ilegal de información	3	3	3	2	5	16	51
3	Uso no autorizado de equipos	2	2	3	2	5	14	50
4	Ausencia de personal	3	3	5	5	3	19	53
5	Fallas en la operación	3	3	5	5	3	19	53
6	Pérdida de información	3	3	3	4	5	18	40
7	Daño físico en documentos	3	4	4	4	5	20	41
8	Daño físico en infraestructura	3	3	5	5	5	21	41
9	Indisponibilidad del PC´s	2	2	4	4	3	15	30
10	Robo de equipos	3	4	2	3	4	16	10
11	Virus	3	4	5	3	4	19	14
12	Modificación de la información	3	5	2	3	3	16	16

ID	Escenarios de Riesgos	VALORACIÓN DEL ESCENARIO DEL RIESGO						
		Multas	Pérdida de credibilidad	Afectación operativa	Pérdida financiera	Pérdida de Información	VALORACION	Promedio de No. De Activos y valoración
13	Destrucción de equipos	3	3	4	2	4	16	20
14	Pérdida de servicios esenciales	3	3	5	4	3	18	21
15	Indisponibilidad general de la sede	3	3	5	4	3	18	10
16	Escucha fraudulenta	3	3	1	3	4	14	8
17	Divulgación de la información	4	5	1	3	3	16	24
18	Indisponibilidad de la base de datos	1	3	5	3	4	16	16
19	Falla de potencia	3	3	5	4	4	19	21
20	Copia fraudulenta de información	3	4	1	4	3	15	8
21	Indisponibilidad de TI	3	3	5	4	4	19	10
22	Error en uso	1	2	4	3	4	14	8
23	Abuso de derechos	3	3	2	3	4	15	8
24	Falla de la aplicaciones críticas	4	3	5	5	5	22	18
25	Indisponibilidad de la red	3	3	5	4	4	19	17
26	Robo de medios	3	3	2	3	5	16	9

Fuente: El Autor.

10.6 MAPAS DE RIESGOS

En la siguiente tabla se muestra para cada casilla el producto de la probabilidad por el impacto: por ejemplo, si el impacto es 5 y la probabilidad también, obtenemos de nivel de riesgo 25 que es equivalente al 100%, ya que este es el máximo valor posible.

Los diferentes escenarios de riesgo identificados para el IMN serán ubicados en los diferentes mapas de riesgo dependiendo, sí es el riesgo inherente, actual o el residual.

Los escenarios de riesgo que tangan mayor probabilidad e impacto estarán ubicados en el mapa de riesgos, en la esquina superior derecha. Estos riesgos deben ser tratados de manera perentoria.

Tabla 38: Matriz de Probabilidad vs. Impacto

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Grave (5)
Certeza (5)	Alto (5)	Alto (10)	Extremo (15)	Extremo (20)	Extremo (25)
Probable (4)	Moderado (4)	Alto (8)	Alto (12)	Extremo (16)	Extremo (20)
Posible (3)	Bajo (3)	Moderado (6)	Alto (9)	Extremo (12)	Extremo (15)
Raro (2)	Bajo (2)	Bajo (4)	Moderado (6)	Alto (8)	Extremo (10)
Improbable (1)	Bajo (1)	Bajo (2)	Moderado (3)	Alto (4)	Alto (5)

Fuente: El Autor.

A continuación se presenta el mapa de Riesgo Inherente:

Tabla 39: Riesgo Inherente

RIESGO INHERENTE					
PROBABILIDAD	IMPACTO				
	Insignificante	Menor	Moderado	Mayor	Grave
Certeza					
Probable					
Posible	10, 26, 21	19, 11	9	6, 7	
Raro	23, 16, 20, 22	13, 18, 25	17		3, 5
Improbable	15	12, 14, 24		8	1, 2, 4

Fuente: El Autor.

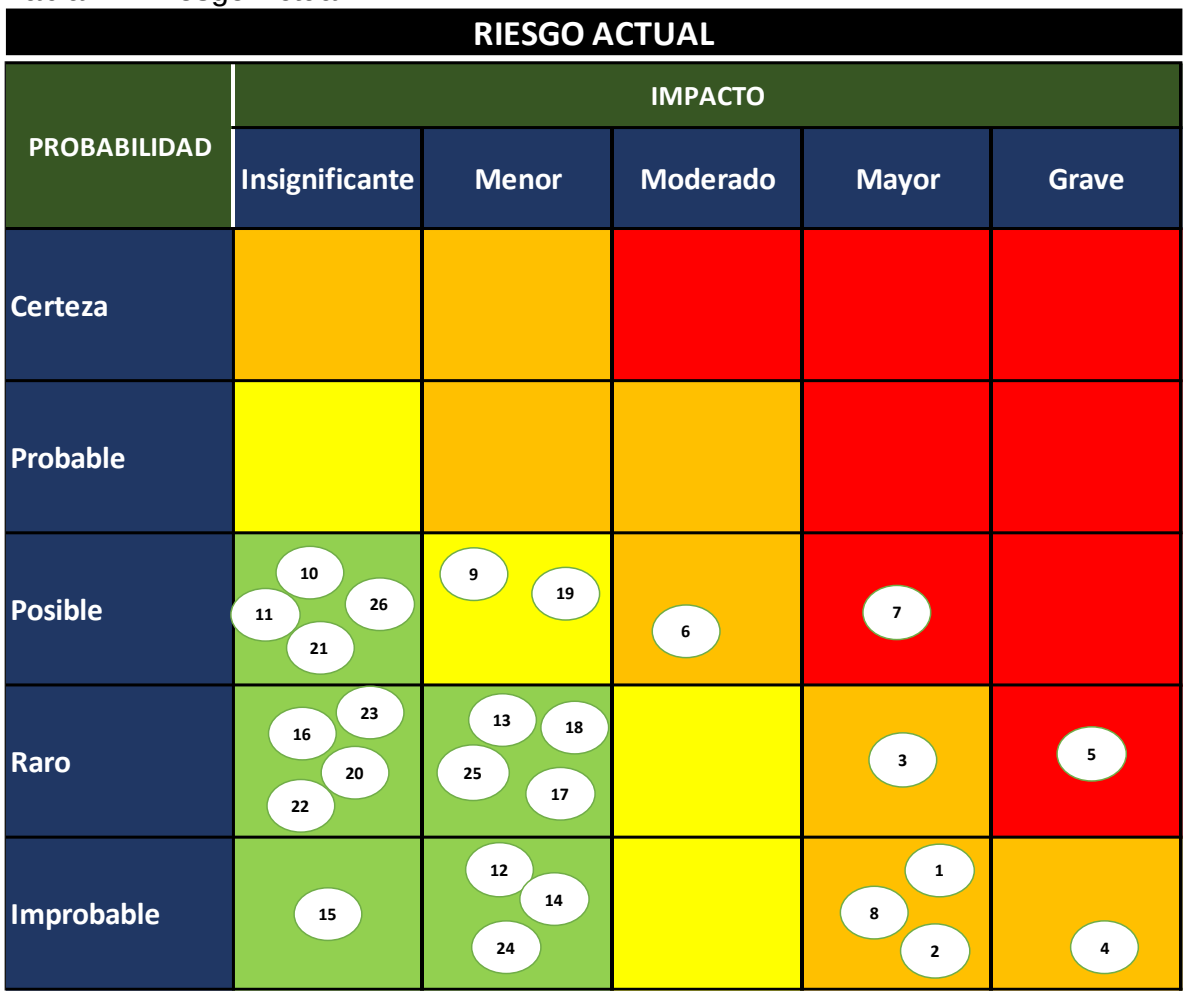
Tabla 40: Total riesgos inherentes

Riesgos Extremos	**4**
Riesgos Altos	**5**
Riesgos Moderados	**3**
Riesgos Bajos	**14**
TOTAL RIESGOS	**26**

Fuente: El Autor.

A continuación se presenta el mapa de Riesgo Actual:

Tabla 41: Riesgo Actual



Fuente: El Autor.

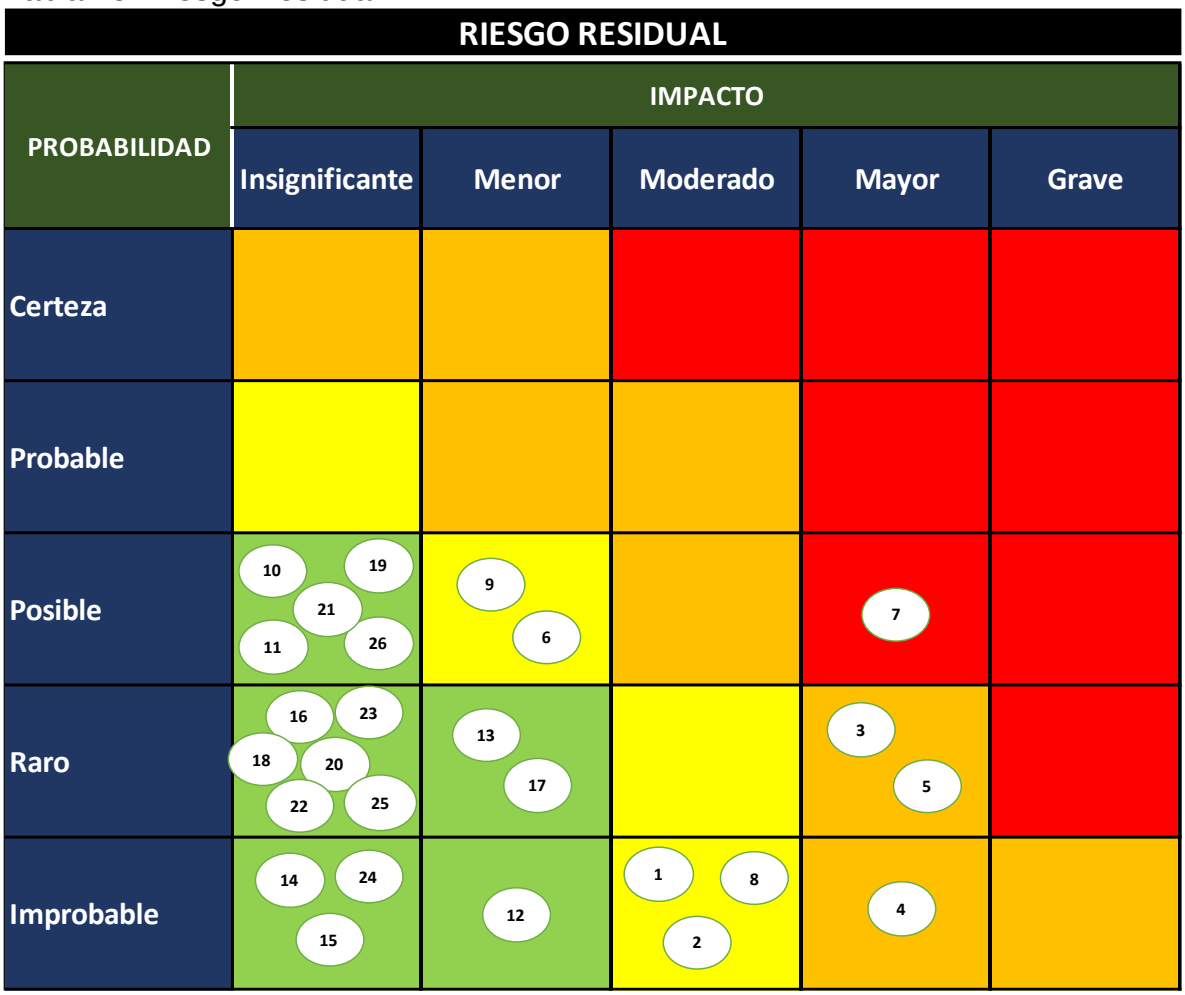
Tabla 42: Total riegos actuales

Riesgos Extremos	**2**
Riesgos Altos	**6**
Riesgos Moderados	**2**
Riesgos Bajos	**16**
TOTAL RIESGOS	**26**

Fuente: El Autor.

A continuación se presenta el mapa de Riesgo Residual:

Tabla 43: Riesgo Residual



Fuente: El Autor.

Tabla 44: Total riego residual

Riesgos Extremos	**1**
Riesgos Altos	**3**
Riesgos Moderados	**5**
Riesgos Bajos	**17**
TOTAL RIESGOS	**26**

Fuente: El Autor.

10.7 CONTROLES RECOMENDADOS Y PRIORIDADES

Se recomiendan controles para las vulnerabilidades que se encontraron durante el desarrollo de las entrevistas, revisión documental y análisis de vulnerabilidades. Para esto nos apoyamos en mejores prácticas internacionales tales como ISO 27001, ISO 27005, ITIL v3, COBIT 5.0, EIA-TIA 942, NFPA 75, entre otras. A estos controles se le asigna una prioridad que depende del riesgo residual calculado. Estas prioridades serán utilizadas para la elaboración del plan de tratamiento de riesgos del IMN.

Tabla 45: Controles y prioridades recomendados

ID	Escenarios de Riesgos	CONTROLES RECOMENDADOS	Prioridad
7	**Daño físico en documentos**	Protección física y respaldo digital según valoración, riesgos y clasificación de la información	Alta
1	**Robo de información**	Uso de metodología, procedimientos y políticas para el desarrollo seguro	Media
2	**Procesamiento ilegal de información**	Procedimientos y estándares formales, usados, documentados y conocidos	Media
9	**Indisponibilidad del PC´s**	Estándares de configuración PC´s	Media
3	**Uso no autorizado de equipos**	Registros (logs) centralizados	Media
4	**Ausencia de personal**	Planes de Continuidad y de Recuperación ante Desastres	Media
5	**Fallas en la operación**	Realización de manera formal y periódica de una gestión de riesgos orientada a activos de información	Media
6	**Pérdida de información**	Establecer Planes de Recuperación ante Desastres (DRP)	Media
8	**Daño físico en infraestructura**	Planes de Continuidad y de Recuperación ante Desastres	Media
19	**Falla de potencia**	Planes de Continuidad y de Recuperación ante Desastres	Media

ID	Escenarios de Riesgos	CONTROLES RECOMENDADOS	Prioridad
10	**Robo de equipos**	Seguridad en el uso de equipos fuera de las instalaciones	Baja
11	**Virus**	Procedimientos y estándares formales, usados, documentados y conocidos	Baja
12	**Modificación de la información**	Realización de manera formal y periódica de análisis de vulnerabilidades y test de penetración.	Baja
13	**Destrucción de equipos**	Mejoramiento de las condiciones físicas y ambientales del centro de cómputo	Baja
16	**Escucha fraudulenta**	Cifrado formal de la información según clasificación y valoración	Baja
17	**Divulgación de la información**	Cifrado formal de la información según clasificación y valoración	Baja
20	**Copia fraudulenta de información**	Cifrado formal de la información según clasificación	Baja
22	**Error en uso**	Sensibilización, entrenamiento, educación y capacitación	Baja
23	**Abuso de derechos**	Entrenamiento en la creación de contraseñas o herramientas automáticas.	Baja
26	**Robo de medios**	Sensibilización, entrenamiento, educación y capacitación	Baja
14	**Pérdida de servicios esenciales**	Establecer Planes de Recuperación ante Desastres (DRP)	Baja
15	**Indisponibilidad general de la sede**	Planes de Continuidad y de Recuperación ante Desastres	Baja
18	**Indisponibilidad de la base de datos**	Establecer Planes de Recuperación ante Desastres (DRP)	Baja
21	**Indisponibilidad de TI**	Establecer Planes de Recuperación ante Desastres (DRP)	Baja
24	**Falla de la aplicaciones críticas**	Establecer Planes de Recuperación ante Desastres (DRP)	Baja
25	**Indisponibilidad de la red**	Gestión de la capacidad y de la disponibilidad.	Baja

Fuente: El Autor.

10.8 PLAN DE TRATAMIENTO

A continuación se presentan las opciones de tratamiento de riesgo a aplicar para cada uno de los riesgos considerados como inaceptables. Se busca seleccionar la opción de control más apropiada para la reducción del riesgo a un nivel aceptable para el IMN. Para cada uno de los controles recomendados, se consideró la prioridad, el tiempo, la complejidad y el costo. Los detalles de la implementación serán estipulados en el documento Plan Estratégico de Seguridad de la Información, PESI.

Tabla 46: Valoración de controles recomendados

CONTROLES RECOMENDADOS	Prioridad	Tiempo estimado de la implementación	Complejidad	Costo
Protección física y respaldo digital según valoración, riesgos y clasificación de la información	Alta	Baja	Baja	Baja
Uso de metodología, procedimientos y políticas para el desarrollo seguro	Media	Baja	Baja	Baja
Procedimientos y estándares formales, usados, documentados y conocidos	Media	Baja	Baja	Baja
Estándares de configuración PC´s	Media	Baja	Baja	Baja
Registros (logs) centralizados	Media	Media	Baja	Media
Planes de Continuidad y de Recuperación ante Desastres	Media	Alta	Alta	Alta
Realización de manera formal y periódica de una gestión de riesgos orientada a activos de información	Media	Alta	Alta	Alta
Establecer Planes de Recuperación ante Desastres (DRP)	Media	Alta	Alta	Alta
Planes de Continuidad y de Recuperación ante Desastres	Media	Alta	Alta	Alta
Planes de Continuidad y de Recuperación ante Desastres	Media	Alta	Alta	Alta
Seguridad en el uso de equipos fuera de las instalaciones	Baja	Baja	Baja	Baja
Procedimientos y estándares formales, usados, documentados y conocidos	Baja	Baja	Baja	Baja
Realización de manera formal y periódica de análisis de vulnerabilidades y test de penetración.	Baja	Baja	Baja	Baja
Mejoramiento de las condiciones físicas y ambientales del centro de cómputo	Baja	Baja	Baja	Baja
Cifrado formal de la información según clasificación y valoración	Baja	Media	Media	Media

CONTROLES RECOMENDADOS	Prioridad	Tiempo estimado de la implementación	Complejidad	Costo
Cifrado formal de la información según clasificación y valoración	Baja	Media	Media	Media
Cifrado formal de la información según clasificación	Baja	Media	Media	Media
Sensibilización, entrenamiento, educación y capacitación	Baja	Media	Media	Media
Entrenamiento en la creación de contraseñas o herramientas automáticas.	Baja	Media	Media	Media
Sensibilización, entrenamiento, educación y capacitación	Baja	Media	Media	Media
Establecer Planes de Recuperación ante Desastres (DRP)	Baja	Alta	Alta	Alta
Planes de Continuidad y de Recuperación ante Desastres	Baja	Alta	Alta	Alta
Establecer Planes de Recuperación ante Desastres (DRP)	Baja	Alta	Alta	Alta
Establecer Planes de Recuperación ante Desastres (DRP)	Baja	Alta	Alta	Alta
Establecer Planes de Recuperación ante Desastres (DRP)	Baja	Alta	Alta	Alta
Gestión de la capacidad y de la disponibilidad	Baja	Alta	Alta	Alta

Fuente: El Autor.

A continuación se presenta el orden recomendado de implementación para cada uno de los diferentes controles propuestos:

Tabla 47: Orden de Implementación

CONTROLES RECOMENDADOS	Orden de Implementación
Protección física y respaldo digital según valoración, riesgos y clasificación de la información	1
Uso de metodología, procedimientos y políticas para el desarrollo seguro	2
Procedimientos y estándares formales, usados, documentados y conocidos	3
Estándares de configuración PC´s	4
Seguridad en el uso de equipos fuera de las instalaciones	5
Procedimientos y estándares formales, usados, documentados y conocidos	6

CONTROLES RECOMENDADOS	Orden de Implementación
Realización de manera formal y periódica de análisis de vulnerabilidades y test de penetración.	7
Mejoramiento de las condiciones físicas y ambientales del centro de cómputo	8
Registros (logs) centralizados	9
Cifrado formal de la información según clasificación y valoración	10
Cifrado formal de la información según clasificación y valoración	11
Cifrado formal de la información según clasificación	12
Sensibilización, entrenamiento, educación y capacitación	13
Entrenamiento en la creación de contraseñas o herramientas automáticas.	14
Sensibilización, entrenamiento, educación y capacitación	15
Planes de Continuidad y de Recuperación ante Desastres	16
Realización de manera formal y periódica de una gestión de riesgos orientada a activos de información	17
Establecer Planes de Recuperación ante Desastres (DRP)	18
Planes de Continuidad y de Recuperación ante Desastres	19
Planes de Continuidad y de Recuperación ante Desastres	20
Establecer Planes de Recuperación ante Desastres (DRP)	21
Planes de Continuidad y de Recuperación ante Desastres	22
Establecer Planes de Recuperación ante Desastres (DRP)	23
Establecer Planes de Recuperación ante Desastres (DRP)	24
Establecer Planes de Recuperación ante Desastres (DRP)	25
Gestión de la capacidad y de la disponibilidad	26

Fuente: El Autor.

Los dominios de la NTC/ISO 27001 que están involucrados con cada uno de los escenarios de riesgo son:

Tabla 48: Dominios de la NTC/ISO 27001 y riesgos

Escenarios de Riesgos	DOMINIOS y CONTROLES ISO 27001:2013 RELACIONADOS CON EL RIESGO													
	D5	D6	D7	D8	D9	D10	D11	D12	D13	D14	D15	D16	D17	D18
Robo de información	x			x	x	x		x	x	x	x	x		
Procesamiento ilegal de información								x						x
Uso no autorizado de equipos					x		x				x			
Ausencia de personal							x						x	
Fallas en la operación								x						
Pérdida de información	x			x	x	x		x	x	x	x	x		
Daño físico en documentos							x							
Daño físico en infraestructura							x						x	
Indisponibilidad del PC´s	x			x			x					x	x	
Robo de equipos				x			x							
Virus	x	x	x		x			x		x	x	x		
Modificación de la información	x			x	x	x		x	x	x		x		
Destrucción de equipos							x							
Pérdida de servicios esenciales				x			x	x	x			x	x	
Indisponibilidad general de la sede							x						x	
Escucha fraudulenta	x			x	x	x			x					
Divulgación de la información	x			x	x	x			x					
Indisponibilidad de la base de datos	x			x	x			x	x				x	
Falla de potencia							x							
Copia fraudulenta de información	x			x	x	x			x					
Indisponibilidad de TI							x	x					x	
Error en uso	x			x	x			x		x				
Abuso de derechos	x			x	x	x		x	x	x		x		
Falla de la aplicaciones críticas										x			x	
Indisponibilidad de la red									x				x	
Robo de medios							x							
Total Dominios seleccionados	**11**	**1**	**1**	**12**	**11**	**7**	**12**	**11**	**10**	**7**	**4**	**7**	**9**	**1**

Fuente: El Autor.

11. FASE 4. PRUEBAS DE VULNERABILIDADES

Esta última fase tiene por tiene por objetivo mostrar las vulnerabilidades y remediaciones de los equipos informáticos propuestos por el IMN. Permitiendo identificar las vulnerabilidades, amenazas a las que está expuesto el instituto y las debilidades en los controles de cada dominio de la ISO.

La fase está basada en las pruebas de seguridad llamadas, ANALISIS DE VULNERABILIDADES, realizadas a las tecnologías de información y comunicaciones.

Toda la información que se muestra a continuación, se ha obtenido lícitamente mediante permisos formales por el IMN. Sus conclusiones son el fruto de un minucioso estudio sobre los resultados de las pruebas. Las técnicas que se explican pueden no ser aplicables directamente en muchos casos.

El análisis de vulnerabilidades facilita la identificación de la brecha de seguridad de la información entre el instituto y el modelo de seguridad de la información MSPI que propone el Ministerio de la información y las comunicaciones MINTIC a través de Gobierno en línea GEL.

Para esta fase se tiene en cuenta la información recolectada y organizada en las anteriores fases por el equipo de seguridad de la información. Dicha información permite reconocer el entorno donde se proyectan los objetivos misionales del instituto.

11.1 SOFTWARE UTILIZADO DURANTE LAS PRUEBAS.

Para la ejecución de las pruebas de hacking ético, el equipo de especialista consultor se apoyó en las siguientes herramientas:

- Analizador de vulnerabilidades “Tenable Nessus ProfessionalFeed”

Esta herramienta es un software utilizado para buscar errores de programación, configuraciones por defecto y vulnerabilidades en equipos informáticos. Algunas de las características claves de la herramienta son:

- Identificar vulnerabilidades de los sistemas operativos instalados.
- Reportar posibles soluciones a las vulnerabilidades encontradas.
- Software ASV por el PCI DSS.
- Software propietario licenciado.
- Base de datos actualizada diariamente por el CVE.

Nmap ("Network Mapper")

Es una herramienta libre y de código abierto utilizada para la exploración de red o de auditoría de seguridad.

Nmap utiliza paquetes IP en bruto en formas novedosas para determinar qué hosts están disponibles en la red, qué servicios (nombre de la aplicación y versión), qué sistemas operativos (OS y versiones) están corriendo, que tipo de filtros o cortafuegos están en uso, y docenas de otras características. Fue diseñado para escanear rápidamente redes muy grandes, pero funciona muy bien contra los equipos independientes.

Nmap se ejecuta en todos los sistemas informáticos operativos principales.

Figura 20: Nmap

Fuente:
https://www.redeszone.net/app/uploads/2013/08/nmap_main.png?x=634&y=309

Distribución para pruebas de seguridad “KALI” y “BackTrack”

KALI y BackTrack son distribuciones GNU/Linux en formato LiveCD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática y hacking ético en general. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la seguridad informática.

Incluye una larga lista de herramientas de seguridad y de hacking listas para usar, entre las que destacan numerosos scanners de puertos y vulnerabilidades, bases de datos de exploits, sniffers, herramientas de análisis forense y herramientas para la auditoría Wireless, entre otras orientas a pruebas de Hacking Ético en todas sus fases.

Figura 21: Kali linux

Fuente: https://www.kali.org/wp-content/uploads/2017/04/kali-release-2017-1.png

Figura 22: Backtrack linux

Fuente: http://www.backtrack-linux.org/

- Otros Software y Distribuciones

Figura 23: Software y distribuciones

Fuente: El autor

Las Bases de Datos consultadas de nuestros ANÁLISIS DE VULNERABILIDADES, se encuentran sustentadas por las siguientes entidades:

Básicamente las pruebas de vulnerabilidad son técnicas aplicadas a las aplicaciones, procesos y usuarios con el fin de comprobar la seguridad de la información en el Instituto.

Existen diferentes técnicas que sirven como marco de referencia para el nivel de seguridad que se evalúa.

11.2 DEFINICIONES

11.2.1 Definición del criterio de criticidad en vulnerabilidades

Para la determinación de criticidad de las vulnerabilidades encontradas se utilizó como base principal el valor de gravedad asignado a cada vulnerabilidad por las herramientas utilizadas en el testing. Posterior a esta calificación inicial (que se presenta dentro de criterios de aceptabilidad definidos en CVSS, documento NISTIR 7435) se llevó a cabo por parte del consultor una prueba directa de explotación de la vulnerabilidad.

Se tuvieron en cuenta vulnerabilidades de clasificación Crítica, Alta, Media y Baja, siendo en últimas la criticidad de éstas determinada principalmente por la percepción del consultor, y estando dicha percepción definida por:

- La explotabilidad efectiva de la vulnerabilidad.
- El vector de acceso necesario para la ejecución de un exploit efectivo.
- La complejidad de programación o de ejecución del ataque.
- El nivel de autenticación requerido para el lanzamiento de un ataque exitoso.
- La disponibilidad de detalles públicos sobre la explotación de la vulnerabilidad.
- El nivel de automatización del proceso de explotación requerido para tener éxito en el aprovechamiento de los hallazgos.

11.2.2 Definiciones escenarios y objetivos

En este módulo se definen los escenarios y objetivos a trabajar durante el desarrollo de las pruebas.

Escenarios

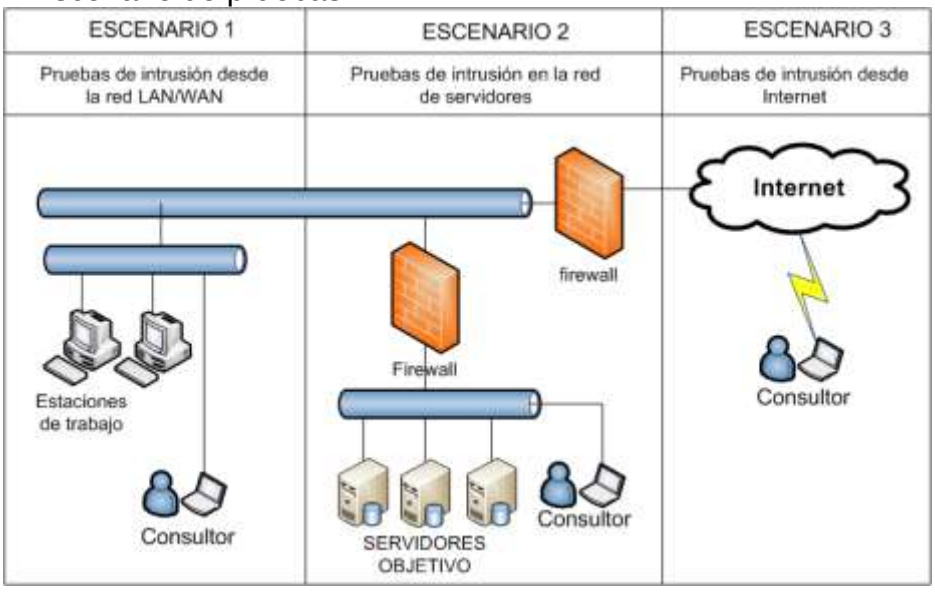
Define los lugares desde donde el consultor realizará las pruebas de seguridad.

Tabla 49: Escenario de pruebas

ESCENARIO	DESCRIPCIÓN	APLICA
Escenario 1	El consultor se encuentra ubicado en un punto de acceso a la red LAN/WAN de la empresa.	SI
Escenario 2	En este lugar, el consultor se encuentra ubicado dentro del firewall que protege el área a ser analizada.	NO
Escenario 3	En este escenario, el consultor realiza las pruebas de seguridad desde una red externa a la empresa. En la mayoría de los casos se hace desde Internet.	NO

Fuente: El autor.

Figura 24: Escenario de pruebas



Fuente: El autor.

11.2.3 Tipo de pruebas de efectividad.

Para este caso aplica la prueba con conocimiento medio del entorno, ya que se posee información limitada o media como algunas direcciones IPs, sistemas operativos, topología de la red, infraestructura del ambiente que será evaluado con el objetivo de realizar un pentesting, simulando un usuario con información básica dentro de la red del Instituto.

11.2.4 Alcance de las pruebas.

En esta etapa se definen reglas específicas antes de ejecutar las pruebas técnicas de efectividad, garantizando que las actividades no afecten la infraestructura y las operaciones del instituto. Para esto se tienen en cuenta los siguientes aspectos:

Plan de Trabajo: en este punto se contempla el tiempo estimado de 60 minutos para realizar las pruebas técnicas a las 4 aplicaciones misionales con más alta probabilidad de ocurrencia contra el impacto materializado con la cual se realiza el análisis de riesgo y el nivel de calificación ALTA mediantes los criterios de Confidencialidad, Integridad y Disponibilidad CID.

Insumos: para las pruebas se requiere listado de los activos de información a evaluar, análisis y valoración de los riesgos, una terminal con acceso a la red interna y externa.

Responsables: el encargado de realizar las pruebas es el ingeniero especialista en seguridad informática de la empresa contratada por licitación pública para el instituto.

Afectaciones posibles: no se afectará la funcionalidad de la operación, ya que las pruebas se realizarán en horario de baja actividad laboral.

Multas o sanciones: no se aplican sanciones disciplinarias o económicas por los incumplimientos de los parámetros mencionados.

Los alcances descritos anteriormente garantizan los acuerdos de servicios con terceros para el control interno en el desarrollo de las pruebas.

11.3 RESULTADOS E IMPACTOS

Mediante el desarrollo de esta monografía de grado, se obtuvo como resultado una visión general acerca del estado actual de la seguridad de la información del instituto, Al consolidar los resultados se pudo determinar que hacen falta varios procedimientos y directriz en la implementación de políticas de seguridad de la información y de controles al igual se debe establecer a qué nivel de cumplimiento se desea llegar y en qué tiempo razonable. Es necesario analizar e implementar el SGSI para proteger los activos de la información del instituto.

El inventario de activos de información del Instituto (IMN) se encuentra desactualizado, por ende no se cuenta con el análisis de riesgos adecuado para el instituto, ya que en el proceso de desarrollo de este proyecto, la evaluación y análisis de brechas se hizo frente a cada requisito especificado en los numerales 4 al 10, puesto que no es aceptable excluir ninguno de ellos.

En el Instituto no se lleva a cabo el 85 % de los controles de la ISO 2700:2013 como se evidencio con los resultados de las entrevistas.

Conforme al puntaje de 21 puntos obtenido por el instituto, el nivel de estratificación de este se encuentra en MEDIO debido a que el personal lleva a cabo el trabajo enfocada en la operación del día a día, y cumple labores en su mayoría REACTIVAS, acatando buenas practicas, pero no existen procesos claros que permitan establecer roles y responsabilidades en los funcionarios del instituto

Tabla 34. Resultado de ingeniería social interna.

INGENERIA SOCIAL				
ITEM	Nivel de inseguridad			
	Critica	Alta	Media	Baja
Control de Acceso Oficinas		X		
Protección de Documentos		X		
Protección de Carnets			X	
Resguardos de Medios			X	
Protección de Escritorio		X		

Fuente: El autor

A continuación se presentan los resultados generales más relevantes de las pruebas técnicas:

- Las vulnerabilidades críticas están focalizadas a la exposición de servicios desactualizados, versiones de componentes obsoletos, falta de parches en el servicio asociados a sistemas operativos WINDOWS.

- En general todos los puertos identificados en los activos tecnológicos se encuentran bien configurados y no arrojan información adicional, el cual pueda colocar en peligro el activo evaluado.

- Falta de actualizaciones en servicio web de tipo APACHE y codificación PHP en aplicaciones WEB internas.

- No es posible administrar activos a través del servicio SSH (puerto22), el cual no permite acceso con credenciales por defecto.

- Se identifican métodos TRACER TRACK en servidores WEB internos.

- Falla en verificación del código JavaScript por parte del Browser, ataques XSS y omisión de herramientas de verificación de Integridad de tablas ARP, Servicio DNS.

- Desde la dirección IP 192.168.1.XX/24 Se publicó un WEB SERVER con funciones JavaScripts maliciosas, se re direccionó el tráfico de consulta de resolución de nombres FQDN para cualquier nombre de dominio, a esta misma maquina después de correr un ataque de DNS Spoofing. El resultado de esta acción obliga a los browsers a visitar el WEB SERVER Malicioso haciendo ZOMBIES a las computadoras de los usuarios.

- Desde la dirección IP 192.168.1.XX/24 después de validar la falta de controles de autenticación de los registros de las tablas ARP de los nodos de la red LAN a través del envío de mensajes ARP gratuitos, Se procede a

ejecutar un ataque de Hombre en medio basado en envenenamiento de tablas ARP.

- Autenticación nula de host vecinos y omisiones en la verificación de integridad de las tablas ARP.

- Fallas a nivel de aplicaciones WEB de tipo XSS, SQL injections y vulnerabilidades críticas a nivel WEB.

- El protocolo SSL, tal como se utiliza en ciertas configuraciones Microsoft Windows y Microsoft Internet Explorer, Mozilla Firefox , Google Chorme, Opera y otros navegadores webs, cifra los datos mediante el modo SBC con vectores de inicialización encadenados, lo cual permite a atacantes man-in-the-middle para obtener las cabeceras HTTP en texto plano por bloques del objetivo elegido para el atacante (BCBA) en una sesión HTTPS, junto con el código JavaScript que utiliza (1) la API de HTML5 WebSocket, (2) la API de Java URLConnection, o (3) el WebClient Silverlight API, también conocido como un ataque “BESTIA”.

  Recomendación: La remediación y soluciones varían según la aplicación y los protocolos TSL versión 1.1 o posteriores no son vulnerables.

11.4 RESULTADOS ANÁLISIS DE VULNERABILIDADES CON ACUNETIX

A continuación se presenta el consolidado de las vulnerabilidades altas, medias, bajas e informativas que se identificaron en los activos de información tecnológicos evaluados a través de la herramienta de escaneo Acunetix empleada para este fin en el Instituto Museo Nacional.

Es de resaltar que los resultados presentados a continuación corresponden a la muestra que se tomó y analizó de los equipos relacionados en el Inventario de activos a evaluar, estos porcentajes no hacen referencia al estado actual de todos los activos de información del instituto.

La actividad programada para el escaneo se lleva a cabo sobre los segmentos los detallados a continuación.

192.168.0.XX/24
192.168.1.XX/24
192.168.X.XX/24
192.168.X.XX/24
192.168.4.XX/24
192.168.5.XX/24
192.168.6.XX/24
192.168.7.XX/24

En el escaneo general de vulnerabilidades realizado en el instituto se encontraron un total de 411 IP's como resultado de esta labor se evidencia que se presentaron 884 vulnerabilidades categorizadas en baja, medias, altas e informativas de esta cantidad total se identifican 75 vulnerabilidades de nivel de riesgo alto con un porcentaje del 13%. 350 vulnerabilidades de nivel de riesgo medio, representado el 62%. 139 vulnerabilidades con un nivel bajo de riesgo con el porcentaje de 25% del total de las vulnerabilidades encontradas en el instituto.

Cabe resaltar que se encontraron 320 vulnerabilidades informativas.

En la siguiente tabla de vulnerabilidades detectadas observamos el resultado de uno de los análisis en forma general.

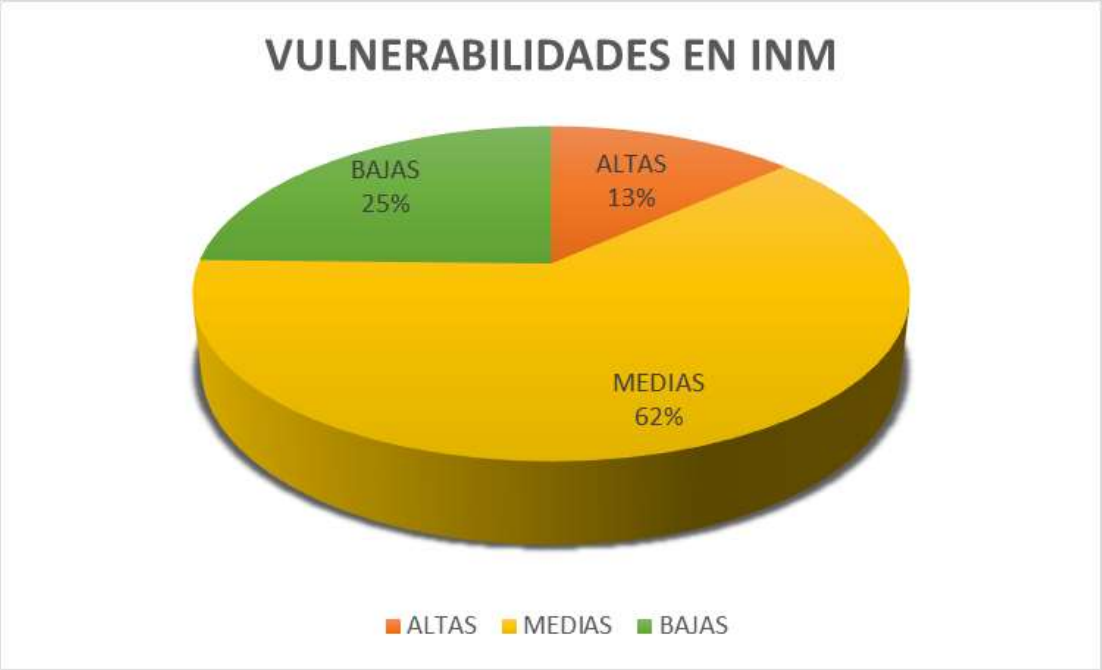
Tabla 50: Vulnerabilidades detectadas

ALTAS	75
MEDIAS	350
BAJAS	139
INFORMATIVAS	320

Fuente: El autor

Seguidamente se aprecia la gráfica con los porcentajes correspondientes a las vulnerabilidades encontradas con cada uno de los riesgos que representan para el instituto, donde se excluye las vulnerabilidades informativas para darle prioridad a los tres principales riesgos con mayor relevancia.

Grafica 4: Vulnerabilidades detectadas en IMN



Fuente: El autor

Teniendo en cuenta lo anterior seguidamente se relacionan las direcciones IP pertenecientes a las terminales que presentan la mayor cantidad de vulnerabilidades de categorización alta y media.

Tabla 51: Terminales con más vulnerabilidades

IP	VULNERABILIDADES
192.168.0.XX	25
192.168.X.XX	10
192.168.X.X0	9
192.168.X.X5	9
192.168.X.9X	8
192.168.2.1X	7
192.168.3.X	7
192.168.X.XX	6
192.168.X.X	6
192.168.X.17	5
192.168.X.X	5
192.168.X.6	5

Fuente: El autor

En los dispositivos de red como los switches se identificó un total de 443 vulnerabilidades de las cuales 59 se categorizaron como vulnerabilidades de nivel de riego alto y medio, lo que corresponde a un 14% del total de hallazgo en esta categoría.

Figura 25: Vulnerabilidades de nivel riesgo alto en las comunicaciones

Vulnerabilidades de Nivel de Riesgo Alto en Comunicaciones		
OpenSSL ASN.1 Parsing Denial Of Service Vulnerability	5	36%
Web Server GET Request Saturation Remote Denial Of Service Vulnerability	1	7%
Web Server HTTP 1.0 Header Denial Of Service Vulnerability	4	29%
Web Server HTTP 1.1 Long Headers Buffer Overflow Vulnerability	1	7%
Web Server HTTP POST Method Remote Buffer Overflow Vulnerability	1	7%
Web Server Long AUTH Header Denial Of Service Vulnerability	1	7%
Web Server Long OPTIONS Header Denial Of Service Vulnerability	1	7%

Fuente: El autor

En la siguiente figura se observa el resultado de uno de los análisis

Figura 26: Resumen de vulnerabilidades en el aplicativo VIGIPAL

Scan information	
Start time	05/10/2016 10:54:27 a. m.
Finish time	05/10/2016 11:04:30 a. m.
Scan time	10 minutes, 3 seconds
Profile	Default

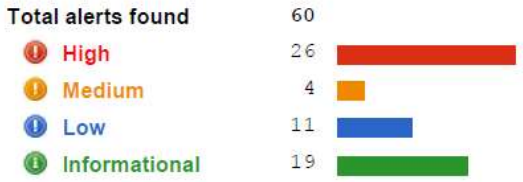
Server information	
Responsive	True
Server banner	Apache/2.4.10 (Debian)
Server OS	Unix
Server technologies	PHP

Threat level

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution



Knowledge base

List of file extensions

File extensions can provide information on what technologies are being used on this website.
List of file extensions detected:

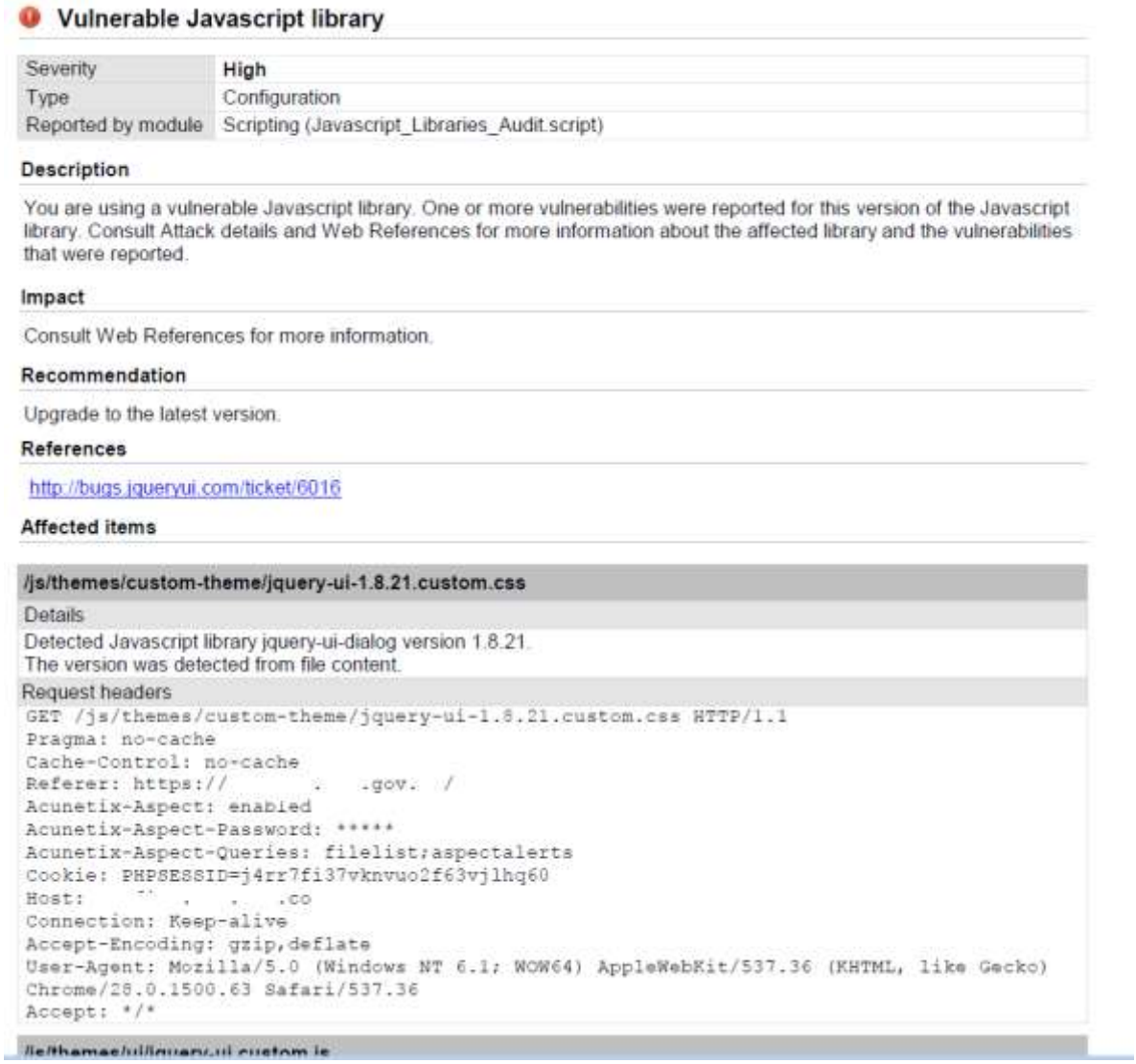
- php => 15 file(s)
- js => 6 file(s)
- css => 3 file(s)

Top 10 response times

The files listed below had the slowest response times measured during the crawling process. The average response time for this site was 245,32 ms. These files could be targetted in denial of service attacks.

Fuente: El autor

Figura 27: Vulnerabilidad alta en el aplicativo VIGIPAL



Vulnerable Javascript library

Severity	**High**
Type	Configuration
Reported by module	Scripting (Javascript_Libraries_Audit.script)

Description

You are using a vulnerable Javascript library. One or more vulnerabilities were reported for this version of the Javascript library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported.

Impact

Consult Web References for more information.

Recommendation

Upgrade to the latest version.

References

http://bugs.jqueryui.com/ticket/6016

Affected items

/js/themes/custom-theme/jquery-ui-1.8.21.custom.css

Details

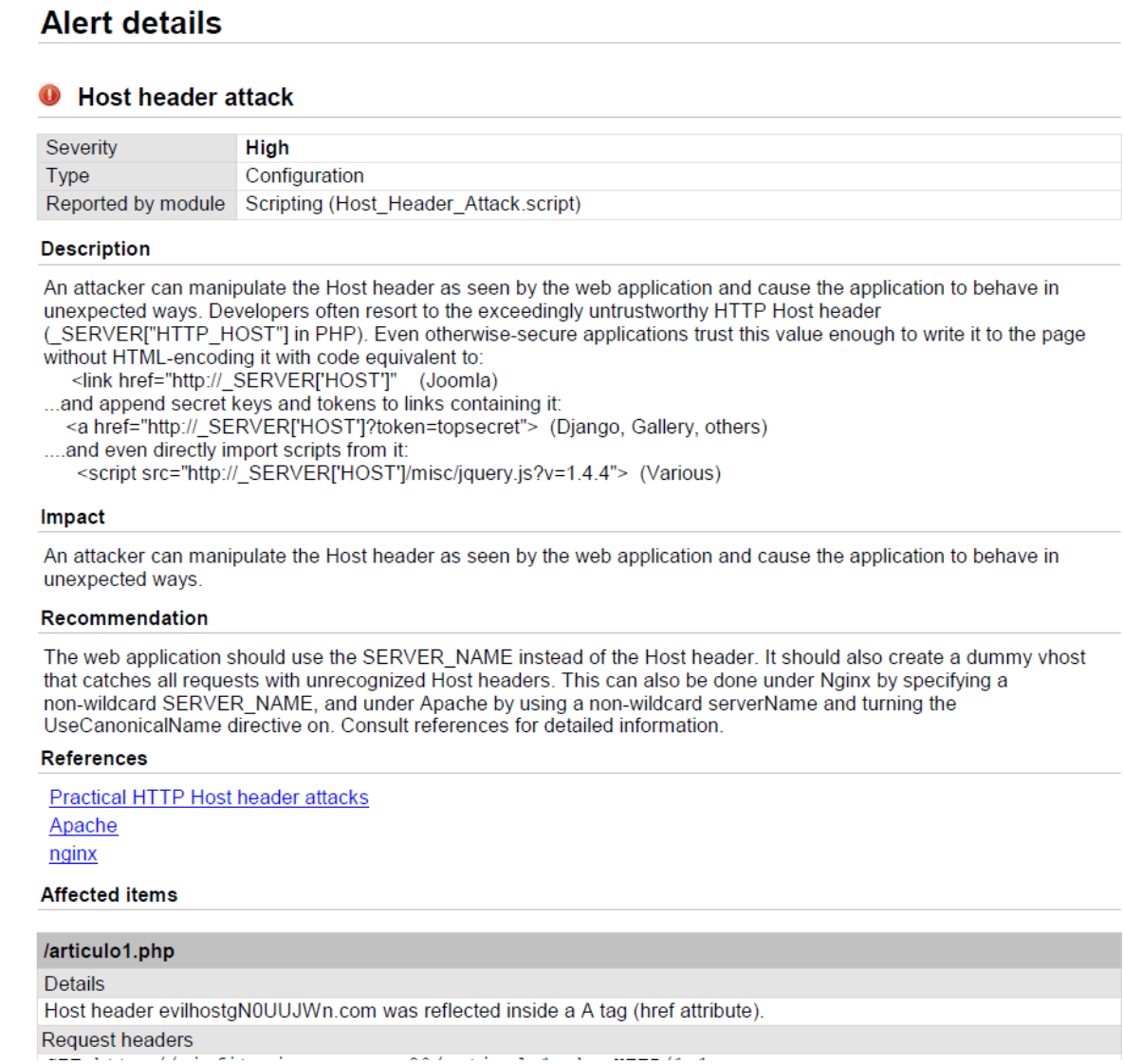
Detected Javascript library jquery-ui-dialog version 1.8.21.
The version was detected from file content.

Request headers

```
GET /js/themes/custom-theme/jquery-ui-1.8.21.custom.css HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://       .   .gov.  /
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=j4rr7fi37vknvuo2f63vjlhq60
Host:      .    .    .co
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Fuente: El autor

Figura 28: Detalles de vulnerabilidad host header attack



Alert details

Host header attack

Severity	**High**
Type	Configuration
Reported by module	Scripting (Host_Header_Attack.script)

Description

An attacker can manipulate the Host header as seen by the web application and cause the application to behave in unexpected ways. Developers often resort to the exceedingly untrustworthy HTTP Host header (_SERVER["HTTP_HOST"] in PHP). Even otherwise-secure applications trust this value enough to write it to the page without HTML-encoding it with code equivalent to:

<link href="http://_SERVER['HOST']" (Joomla)

...and append secret keys and tokens to links containing it:

<a href="http://_SERVER['HOST']?token=topsecret"> (Django, Gallery, others)

....and even directly import scripts from it:

<script src="http://_SERVER['HOST']/misc/jquery.js?v=1.4.4"> (Various)

Impact

An attacker can manipulate the Host header as seen by the web application and cause the application to behave in unexpected ways.

Recommendation

The web application should use the SERVER_NAME instead of the Host header. It should also create a dummy vhost that catches all requests with unrecognized Host headers. This can also be done under Nginx by specifying a non-wildcard SERVER_NAME, and under Apache by using a non-wildcard serverName and turning the UseCanonicalName directive on. Consult references for detailed information.

References

Practical HTTP Host header attacks
Apache
nginx

Affected items

/articulo1.php
Details
Host header evilhostgN0UUJWn.com was reflected inside a A tag (href attribute).
Request headers

Fuente: El autor

12. IMPACTOS

Con el anterior proyecto se pretende dejar totalmente documentado todo el nivel de seguridad y privacidad de la información encontrada al interior del Instituto, como la primera fase de diagnóstico de seguridad para una futura implementación y segunda fase para la implementación del Modelo de Seguridad y Privacidad de La Información.

13. RECOMENDACIONES GENERALES DE MEJORA Y REMEDIACIÓN

A continuación, se enumeran las principales recomendaciones generales para el IMN, como resultado de la ejecución de pruebas técnicas de vulnerabilidades, Pent Testing y pruebas de ingeniería social.

El termino dirección de la organización debe estar contemplado siempre. En las tareas fundamentales del Sistema de Gestión de seguridad y privacidad de la información que la norma ISO 27001 asigna a la dirección donde se detallan los siguientes elementos:

Establecer la política y objetivos de la seguridad de la información y todo el marco normativo para su implantación.

- Integrar los requisitos del Sistema de Gestión de Seguridad de la Información en los procesos de la Institución.

- Disponer los recursos para la implementación y operación del MSPI.

- Asegurar que el SGSI logre los resultados previstos.

- Apoyar otros roles pertinentes de la dirección para demostrar su liderazgo aplicado a sus áreas de responsabilidad.

- Asegurar que las responsabilidades y autoridades de los roles pertinentes a la seguridad de la información se asignen y comuniquen.

Revisar el SGSI del Instituto con el conjunto de actividades planificadas, para asegurarse de su aplicación, adaptación, eficiencia y eficacia continua. Los jefes deben revisar con regularidad el cumplimiento de políticas, aplicación de controles, normas de seguridad adecuadas que garanticen las buenas prácticas.

14. RECOMENDACIONES A NIVEL DE INFRAESTRUCTURA

- Restringir el acceso a las herramientas, consolas de gestión y administración de equipos de comunicaciones, Swhitches, equipos de seguridad, firewall, servidores DELL a usuarios no autorizados en la red interna del IMN.

- Actualización de parches en servidores, servicios de gestión de servidores, DATAPROTECTOR, servidores SAMBA, sistema UNIX.

- Deshabilitar el servicio de terminal servicies si no es utilizado. Si esto no es posible se debe restringir el acceso a estaciones validas, y en ningún caso permitir su acceso desde Internet. Este protocolo es susceptibles a ataques de tipo MAN-in-the-Middle, que permite el robo de credenciales de autenticación a los usuarios válidos.

- Deshabilitar servicio por defecto en servidores y estaciones de usuarios finales.

- Realizar la verificación y eliminación de parámetros por default en la implementación de Bases de datos, dispositivos de comunicaciones y aplicaciones.

- Restringir el acceso remoto por consola, únicamente a direcciones IP autorizadas y plenamente identificadas, teniendo en cuenta la política de perfiles y nivel de acceso para cada usuario.

- Mantener una línea base de seguridad en las plataformas tecnológicas del IMN, el cual permita desarrollar e implementar guías de aseguramiento, benchmarking de seguridad y mejores prácticas de la industria en tecnologías aplicadas en el IMN.

15. RECOMENDACIONES A NIVEL DE SOFTWARE

- Desarrollar e implementar un plan de actualización de todos los sistemas y servicios que se encuentran implementado dentro del IMN.

- Desarrollar e implementar un plan para el cambio periódico de contraseñas y que a su vez se implemente contraseñas robustas.

- Desarrollar pruebas periódicas al código de las aplicaciones, mediante prácticas de desarrollo seguro y/o código seguro en las aplicaciones internas para el instituto.

- Habilitar reglas de acceso para que los usuarios del sistema solo puedan descargar las aplicaciones autorizada con sus respectivas licencias legales desde las páginas o sitios oficiales.

- No permitir que los funcionarios, usuarios internos o externos anoten las contraseñas en ningún documento, ni que sean compartidas con otros usuarios.

- No permitir que los usuarios o funcionarios abran nunca mensajes electrónicos de origen desconocido, sospechosos, ni sus archivos adjuntos.

- No permitir que los usuarios de la red puedan acceder a sitios o páginas web de dudosa credibilidad o sin certificado de seguridad y confianza.

16. RECOMENDACIONES A NIVEL DE APLICACIONES

Filtrar SERVICIOS WEB por defecto, los cuales puedan estar expuesto al internet

Revisar y actualizar la configuración de los certificados SSL internos, detectados en aplicaciones de administración y seguridad, debido a que la configuración actual, permite la detección de múltiples vulnerabilidades que afectan al protocolo y cifrado de las aplicaciones.

Realizar pruebas controladas para validar si se puede deshabilitar el servicio / protocolo SSL y habilitar TLS; esto debido a que hoy en día se han detectado diversas vulnerabilidades sobre el protocolo SSL.

Hacer uso de protocolo cifrados o actualizar los ya existes como SSL o SSH en la comunicación con el servidor o dispositivos, con el fin de evitar la intercepción de información sencilla cuando esta sea trasmitida en texto plano, por ejemplo en donde se requiere ingresar credenciales de usuario.

17. RECOMENDACIONES A NIVEL DE INGENIERÍA SOCIAL

Implementar una política de contraseñas seguras a nivel del IMN para la gestión y la administración de los equipos tecnológicos

Desarrollar campañas de concientización sobre seguridad informática y de la información a todo el personal que se encuentra laborando en el instituto

Se recomienda realizar monitoreo y auditorias periódicas a los sistemas de vigilancia como cámaras o sistemas de CCTV que posee el Instituto.

Se debe concientizar a los usuarios legítimos de las diferentes dependencias del comportamiento que deben permitir en sus áreas de trabajo y los comportamientos que deben ser notificados de inmediato al jefe del grupo de seguridad y generar la conciencia para que estos sean los principales custodios de la información contenida en los equipos y archivos dentro de las áreas restringidas.

Establecer políticas de cierre de sesión por inactividad y bloqueo del protector de pantalla para todos los computadores del instituto tanto como para estaciones de trabajo y servidores.

Seleccionar muy bien el papel al ser reciclado que este no contenga información que pueda utilizar cualquier atacante, de lo contrario realizar la respectiva destrucción.

A nivel externo se recomienda a los funcionarios no revelar información confidencial o sensible del Instituto a través de correos anónimos, llamadas, o aplicaciones sospechosas o cualquier actividad inusual.

18. CONCLUSIONES

Uno de los riegos de incidentes de seguridad de la información más altos para el Instituto (INM) es el área de recursos humanos debido a que la mayoría de funcionarios no están capacitados en los temas de seguridad informática, sobre todo el personal del área de desarrollo de aplicaciones lo cual no permite que realicen actividades de desarrollo seguro aplicando buenas practicas.

Para el análisis de los resultados presentados en actual escaneo frente al desarrollo de las pruebas de vulnerabilidades anterior donde no se tuvieron en cuenta los dispositivos categorizados como impresoras y teléfonos, los resultados arrojados de las dos actividades donde se tuvo en cuenta el mismo alcance se relacionan en la siguiente tabla:

Tabla 52: Resultados comparativos con anterior escaneo

Escaneo	Cantidad de direcciones IP	Nivel de Riesgo de las vulnerabilidades presentadas				
		Alto	Medio	Bajo	Informativo	Total
Anterior	409	71	345	118	328	862
Actual	411	75	350	139	320	884
Diferencia	2	4	5	21	-8	22

Fuente: El autor

Como se evidencia en la anterior tabla de resultados comparativos existe un índice de crecimiento de vulnerabilidades en 3 meses aproximadamente.

Entre otras conclusiones se mencionan las siguientes:

- La información es uno de los activos más importantes.
- Se debe preservar la confidencialidad, la integridad y disponibilidad de la información.
- La gerencia debe hacer de la seguridad de la información parte del Instituto.
- La seguridad no es un producto es un proceso.
- Los ataques cibernéticos van en aumento y son cada vez más sofisticado.
- Se beben utilizar antivirus y buenas contraseñas.
- Se bebe crear una cultura en seguridad de la información.
- La seguridad es tan fuerte como el punto más débil.

19. DIVULGACIÓN

Para el cumplimiento de la actividad de divulgación donde se presentarán los resultados obtenidos en el proyecto, se determinó programar una capacitación en la sala de juntas de la gerencia en dos jornadas a todos los funcionarios y directivos del Instituto.

En la capacitación se socializarán los conceptos y diferencias entre seguridad informática, seguridad de la información, seguridad de la infraestructura física y seguridad de los recursos humanos; resaltando la importancia de recordar que la información está en muchos medios o partes, para poder identificar y aplicar bien cada uno de los términos cuando sea necesario. También se aclarará la definición de ethical hacking con la presentación del ingeniero especialista a cargo de las pruebas técnicas y pruebas de ingeniería social.

Las entidades del gobierno están obligadas a desarrollar programas de ciberseguridad y ciberdefensa que permitan garantizar la capacidad del estado para gobernar y seguir prestando de manera continua sus servicios en línea a la ciudadanía. Los conceptos de ciberseguridad y ciberdefensa están estrechamente relacionados con la seguridad de la información, seguridad informática y la continuidad del negocio. La ciberseguridad no es otra cosa que la evolución natural del uso de las tecnologías de la información con la respuesta que debe tener las entidades gubernamentales frente a los riegos derivados de su uso y apropiación.

En el desarrollo de esta capacitación es importante y fundamental que cada uno de los participantes del Instituto reconozca los siguientes principios:

- La gerencia debe tener prioridad con los temas de ciberseguridad como un riesgo que afecta a toda el Instituto.

- Los asesores jurídicos deben comprender las afectaciones legales de cada uno de los riesgos cibernéticos y la relación actual con el Instituto.

- El grupo de gestión debe tener conocimiento sobre los aspectos relacionados con la ciberseguridad con el debido espacio y nivel de importancia en la agenda para tratar los temas de manera adecuada.

- La alta gerencia debe disponer de todos los recursos económicos, humanos, tecnológicos, y de tiempo.

- La alta gerencia junto con cada uno de los jefes o coordinadores de los procesos deben establecer el nivel de riesgo cibernético aceptable, con sus criterios para darle tratamiento (evitar, aceptar, mitigar, transferir).

Teniendo en cuenta los resultados de las pruebas aplicadas al instituto se le recomienda que se apropie de un Framework reconocido y de aceptación internacional que permita desarrollar un programa solido eficaz, eficiente y medible para impulsar la evolución de la ciberseguridad en el Instituto contando con la capacidad de identificar, soportar y supervivir a un ciberataque garantizando el plan de continuidad sin afectar a los ciudadanos.

Debido a esto se hace necesario dar continuidad al programa de concientización de los usuarios tanto internos como externos para apoyar la modificación de aptitudes y percepciones, tanto organizacional como personal. De esta forma se enfatiza en la importancia de la seguridad, se demuestran los grandes problemas que acarrea el desconocimiento o la desobediencia de las normas de seguridad y los riesgos a los que se encuentra expuesto el Instituto y la necesidad de entrenamiento en el reconocimiento y reporte de incidentes de seguridad de la información.

Por otra para obtener mayor apoyo y compromiso de la alta gerencia es importante ampliar el entendimiento antes los riesgos a los que se encuentra expuesto el Instituto y que pueden impedir el buen desarrollo de su misión y afectar su imagen pública como instituto gubernamental.

Finalizada la capacitación se realizará:

- Firma de planilla de asistencia.

- Retroalimentación en forma de test a cada uno de los participantes para evaluar los conocimientos adquiridos.

- Entrega de un incentivo por la asistencia y participación.

20. BIBLIOGRAFÍA

ISO 27001.ES Sistema de Gestión de la Seguridad de la información, 2012. Disponible en http://www.iso27000.es. [En línea]

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES Estrategia De Gobierno en Guía 5 Para la Gestión y Clasificación de Activos de Información 2016. Disponible en http://mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_clasificacion.pdf. [En línea]

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES Estrategia De Gobierno En Línea Articulo 8253 Modelo de Seguridad, 2016. Disponible en http://mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf. [En línea]

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES Estrategia De Gobierno en Línea Guía 7 de Gestión de Riesgos 2016. Disponible en http://mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf. [En línea]

VILLALON, Antonio. Seguridad Unix y Redes version 2.1 España. Julio 2002 Disponible en : http://gseguridad.unicauca.edu.co/articulos/unixsec.pdf.

ANEXO A. REGISTRÓ DE ACTIVOS DE INFORMACIÓN

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS **Versión 1.0**

CATEGORÍA DE INFORMACIÓN	PUBLICADO	REGISTRO DISPONIBLE PARA SER SOLICITADO POR EL PÚBLICO	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
CIRCULARES	SI	http://www.Gerenteia.gov.co/	Circulares	Ciculares Reglamentaris, informativas e instructivas ordenadas por orden consecutivo	Español	Físico/Digital	Papel y PDF	http://www.Gerenteia.gov.co/web/guest/circulares
CONVENIOS CON ENTIDADES PRIVADAS Y OFICIALES	NO	SI	Convenios con entidades privadas y oficiales	Acuerdos de la CGR con otras entidades	Español	Físico	Papel	Archivo de Gestión del Despacho del Gerente General, es de consulta solo para las partes que firman el convenio
GESTIÓN CONSECUTIVA DEL DESPACHO	NO	SI	Gestión consecutiva del despacho	Comunicaciones oficiales Internas o externas enviadas, ordenadas en forma consecutiva	Español	Físico	Papel	Archivo de Gestión del Despacho del Gerente General
INVITACIONES Y EVENTOS PARA Gerente GENERAL	NO	SI	Invitaciones y eventos para Gerente General	Comunicaciones oficiales informado sobre eventos donde se solicita la participación del Gerente	Español	Físico	Papel	Archivo de Gestión del Despacho del Gerente General
SOLICITUDES RELACIONADAS CON PROCESOS TRIBUNALES	NO	N/A	Solicitudes relacionadas con procesos tribunales	Comunicaciones relacionadas con procesos	Español	Físico	Papel	Archivo de Gestión del Despacho del Gerente General
COMUNICACIONES INFORMATIVAS	NO	SI	Comunicaciones informativas	Comunicaciones oficiales recibidas, ordenadas en forma consecutiva	Español	Físico - Papel	Papel	Archivo de Gestión de Secretaría Privada
GESTIÓN CONSECUTIVA SECRETARIA PRIVADA	NO	SI	Gestión consecutiva de Secretaría Privada	Comunicaciones oficiales Internas o externas enviadas, ordenadas en forma consecutiva	Español	Físico - Papel	Papel	Archivo de Gestión de Secretaría Privada
ACTAS DE COMITÉ INTERNO	NO	SI	Actas de comité interno	Actas de seguimiento a actuaciones procesales - Acciones de PMI y PA	Español	Físico	Documento texto	Archivo de Gestión de la Unidad de Investigaciones Especiales Contra la Corrupción
ACTUACIONES ESPECIALES DE CONTROL FISCAL	NO	SI	Actuaciones especiales de control fiscal	El desarrollo de las actuaciones especiales declaradas de impacto nacional 2012-2013	Español	Físico	Documento texto	Archivo de Gestión de la Unidad de Investigaciones Especiales Contra la Corrupción
INFORMES SOBRE GESTIÓN FISCAL	NO	SI	Informes sobre gestión fiscal	Informes resultado de las actuaciones especiales	Español	Físico	Documento texto	Archivo de Gestión de la Unidad de Investigaciones Especiales Contra la Corrupción
CONSULTAS DE INFORMACIÓN DE OTRAS AUTORIDADES DE CONTROL, INSPECCIÓN Y VIGILANCIA	NO	SI	Consultas de información de otras autoridades de control, inspección y vigilancia	Consultas de información de actuaciones especiales de autoridades diferentes	Español	Físico	Documento texto	Archivo de Gestión de la Unidad de Investigaciones Especiales Contra la Corrupción
ACTUACIONES ESPECIALES DE FISCALIZACIÓN	NO	SI	Actuaciones especiales de fiscalización	El desarrollo de las actuaciones especiales declaradas de impacto nacional	Español	Físico	Documento texto	Archivo de Gestión de la Unidad de Investigaciones Especiales Contra la Corrupción
AUTOS DE IMPACTO NACIONAL	NO	SI	Autos de impacto nacional	Autos mediante los cuales se declaran hechos o Procesos de Responsabilidad Fiscal de impacto nacional para ser tramitados por la Unidad de Investigaciones Especiales Contra la Corrupción	Español	Físico	Documento texto	Archivo de Gestión de la Unidad de Investigaciones Especiales Contra la Corrupción
CONSULTAS SOBRE ANTECEDENTES	NO	SI	Consultas sobre antecedentes	Consultas de información sobre antecedentes tramitados en la Unidad de Investigaciones Especiales Contra la Corrupción	Español	Físico	Documento texto	Archivo de Gestión de la Unidad de Investigaciones Especiales Contra la Corrupción
CONSULTAS SOBRE INDAGACIONES PRELIMINARES	NO	SI	Consultas sobre indagaciones preliminares	Consultas de información sobre Indagaciones Preliminares tramitados en la Unidad de Investigaciones Especiales Contra la Corrupción	Español	Físico	Documento texto	Archivo de Gestión de la Unidad de Investigaciones Especiales Contra la Corrupción
CONSULTAS SOBRE PROCESOS DE RESPONSABILIDAD FISCAL	NO	SI	Consultas sobre procesos de responsabilidad fiscal	Consultas de información sobre Procesos de Responsabilidad Fiscal tramitados en la Unidad de Investigaciones Especiales Contra la Corrupción	Español	Físico	Documento texto	Archivo de Gestión de la Unidad de Investigaciones Especiales Contra la Corrupción
CONTROL DE ENTREGA DE COMUNICACIONES OFICALES	NO	SI	Control de entrega de comunicaciones oficiales	Planillas y libros de registro de entrega de comunicaciones oficiales	Español	Físico	Documento texto	Archivo de Gestión de la Unidad de Investigaciones Especiales Contra la Corrupción
DERECHOS DE PETICIÓN	NO	SI	Derechos de petición	Derechos de petición - Solicitudes de información	Español	Físico	Documento texto	Archivo de Gestión de la Unidad de Investigaciones Especiales Contra la Corrupción
INFORMES AL CONGRESO Y/O PRESIDENTE DE LA REPÚBLICA	NO	SI	Informes al Congreso y/o Presidente de la República	Informe de gestión de la Unidad de Investigaciones Especiales Contra la Corrupción de acuerdo a los requerimientos de la Oficina de Planeación	Español	Físico	Documento texto	Archivo de Gestión de la Unidad de Investigaciones Especiales Contra la Corrupción
INFORMES DE AUDITORÍA EXTERNA	NO	SI	Informes de auditoría externa	Documentos relacionados con las auditorias adelantadas por la AGR (solicitudes- observaciones - respuestas)	Español	Físico	Documento texto	Archivo de Gestión de la Unidad de Investigaciones Especiales Contra la Corrupción
INFORMES DE COMISIONES DE SERVICIO	NO	SI	Informes de comisiones de servicio	Informes de cumplido de las comisiones de los funcionarios de la Unidad de Investigaciones Especiales Contra la Corrupción	Español	Físico	Documento texto	Archivo de Gestión de la Unidad de Investigaciones Especiales Contra la Corrupción

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS								Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
INFORMES DE DELEGACIONES	NO	SI	Informes de delegaciones	Informes relacionados con los contratos de prestación de servicios	Español	Físico	Documento texto	Archivo de Gestión de la Unidad de Investigaciones Especiales Contra la Corrupción
INFORMES DE GESTIÓN	NO	SI	Informes de gestión	Informes relacionados con la gestión de la Unidad de Investigaciones Especiales Contra la Corrupción	Español	Físico	Documento texto	Archivo de Gestión de la Unidad de Investigaciones Especiales Contra la Corrupción
INFORMES DE RENDICIÓN DE LA CUENTA	NO	SI	Informes de rendición de la cuenta	Informes - Comunicaciones - Actas - Formatos relacionados con la rendición de la cuenta a la AGR	Español	Físico	Documento texto	Archivo de Gestión de la Unidad de Investigaciones Especiales Contra la Corrupción
INFORMES SOBRE EL ESTADO DE LAS INVESTIGACIONES	NO	NO	Informes sobre el estado de las investigaciones	Informe del estado de las Indagaciones Preliminares y Procesos de Responsabilidad Fiscal Ordinarios - Verbales para la alta dirección	Español	Físico	Documento texto	Archivo de Gestión de la Unidad de Investigaciones Especiales Contra la Corrupción
LIBROS RADICADORES	NO	SI	Libros radicadores	Libros donde se radican los oficios de asignación- Autos de impacto- Trámites de Secretaria Común	Español	Físico	Documento texto	Archivo de Gestión de la Unidad de Investigaciones Especiales Contra la Corrupción
NOTIFICACIONES POR ESTADO	NO	SI	Notificaciones por estado	Notificaciones por estado	Español	Físico	Documento texto	Archivo de Gestión de la Unidad de Investigaciones Especiales Contra la Corrupción
OFICIOS DE ASIGNACIÓN	NO	SI	Oficios de asignación	Oficios mediante los cuales se asignan las actuaciones declaradas de impacto nacional	Español	Físico	Documento texto	Archivo de Gestión de la Unidad de Investigaciones Especiales Contra la Corrupción
PROCESOS ADMINISTRATIVOS SANCIONATORIOS FISCALES	NO	SI	Procesos Administrativos Sancionatorios Fiscales	Trámite de procesos administrativos sancionatorios de acuerdo a lo establecido en el Artículo 101 de la Ley 42 de 1993 (2012)	Español	Físico	Documento texto	Archivo de Gestión de la Unidad de Investigaciones Especiales Contra la Corrupción
PROYECTOS DE RESOLUCIONES DE COMISIONES	NO	SI	Proyectos de resoluciones de comisiones	Resoluciones de comisión de los funcionarios de la Unidad de Investigaciones Especiales Contra la Corrupción	Español	Físico	Documento texto	Archivo de Gestión de la Unidad de Investigaciones Especiales Contra la Corrupción
COMUNICACIONES INFORMATIVAS			Comunicaciones informativas	Comunicaciones oficiales con carácter informativo	Español	Físico	Documento de texto	Archivo de gestión de la Unidad de Cooperación Nacional e Internacional de Prevención, Investigación e Incautación de Bienes
CONVENIOS INTERNACIONALES			Convenios Internacionales	Convenios suscritos entre la CGR y entidades internacionales	Español	Físico	Documento de texto	Archivo de gestión de la Unidad de Cooperación Nacional e Internacional de Prevención, Investigación e Incautación de Bienes
CONTROL EXCEPCIONAL	Controles Excepcionales	Expediente	ERxxx_Año_Senado /Cámara_CE_Congresista_tema_región	Resumen temático de solicitud de cada control excepcional por solicitud de las Comisiones Constitucionales Permanentes del Congreso	Español	Físico/Digital	Excel/Pdf	Se publica registro básico en web por período legislativo, pero está disponible para ser solicitada copia de expediente digital al Jefe de la Unidad
DENUNCIA	Denuncias Cámara	Expediente	ERxxx_Año_Camara_Denuncia_Representante_Tema_Región	Resumen temático de denuncias presentadas por los Representantes a la Cámara	Español	Físico/Digital	Excel/Pdf	Se publica registro básico en web por período legislativo, pero está disponible para ser solicitada copia de expediente digital al Jefe de la Unidad
DERECHOS DE PETICIÓN_SOLICITUD	Derechos de Petición	Expediente	ERxxx_Año_Camara_DP/Solicitud_Representante_Tema_Región	Resumen temático de derechos de petición o solicitudes de información presentadas por los Representantes a la Cámara, las comisiones o la Plenaria de la Cámara de Representantes.	Español	Físico/Digital	Excel/Pdf	Se publica registro básico en web por período legislativo, pero está disponible para ser solicitada copia de expediente digital al Jefe de la Unidad
INVITACIONES	Invitaciones Cámara	Expediente	ERxxx_Año_Camara_Invitación_Plenaria/Comisión_Proposición_Tema_Representante	Resumen temático de invitaciones a la CGR a audiencias, foros o debates por los presentadas por los Representantes a la Cámara, las comisiones o la Plenaria de la Cámara de Representantes.	Español	Físico/Digital	Excel/Pdf	Se publica registro básico en web por período legislativo, pero está disponible para ser solicitada copia de expediente digital al Jefe de la Unidad
DENUNCIA	Denuncias Senado	Expediente	ERxxx_Año_Senado_Denuncia_Senador_Tema_Región	Resumen temático de denuncias presentadas por los Senadores de la República.	Español	Físico/Digital	Excel/Pdf	Se publica registro básico en web por período legislativo, pero está disponible para ser solicitada copia de expediente digital al Jefe de la Unidad
DERECHOS DE PETICIÓN_SOLICITUD	Derechos de Petición o	Expediente	ERxxx_Año_Senado_DP/Solicitud_Senador_Tema_Región	Resumen temático de derechos de petición o solicitudes de información presentadas por los Senadores, las comisiones o la Plenaria del Senado de la República.	Español	Físico/Digital	Excel/Pdf	Se publica registro básico en web por período legislativo, pero está disponible para ser solicitada copia de expediente digital al Jefe de la Unidad

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS **Versión 1.0**

CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
INVITACIONES	Invitaciones Senado	Expediente	ERxxx_Año_Senado_Invitación_Plenaria/Comisión_Proposición_Tema_Senador	Resumen temático de invitaciones a la CGR a audiencias, foros o debates por los presentadas por los Senadores, las comisiones o la Plenaria del Senado de la República.	Español	Físico/Digital	Excel/Pdf	Se publica registro básico en web por período legislativo, pero está disponible para ser solicitada copia de expediente digital al Jefe de la Unidad
INFORMES SOBRE ANÁLISIS DE PROYECTOS DE LEY Y ACTOS LEGISLATIVOS	Analisis de	Texto de Análisis a PL y PAL	Análisis_PL/PAL_XXX_C/S_Año_Tema	Resumen temático de cada análisis de PL ó PAL efectuado	Español	Digital	Pdf	Se publican registros web por período legislativo con links a cada análisis efectuado
MEMORANDOS	Memorandos	Memorandos y anexos	80013_Consecutivo_Año_Tema	Resumen temático de cada memorando UATC	Español	Digital	Pdf	Se públican registros web con links a cada Memorando Generado por la UATC
ACTAS	Documento	Archivo de Gestión de la USATI	Actas de entrega de dependencia, Acta de entrega de documentos por novedades de personal	Actas, copia de inventario físico, relación de talento humano, copia de registro del SIREP, relación de carga laboral por equipo y/o funcionario, formato único de inventario documental, certificación GRE-8115-AX-23 y 24, comunicaciones oficiales	Español	Físico y/o Electronico	Tiff Sigedoc y/o físico	Disponible Archivo Gestión USATI
COMUNICACIONES INFORMATIVAS	Documento	Archivo de Gestión de la USATI	Comunicaciones oficiales de carácter informativo	Comunicaciones oficiales de carácter informativo	Español	Físico y/o Electronico	Tiff Sigedoc y/o físico	Disponible Archivo Gestión USATI
CONTROL DE ASISTENCIA	Documento	Archivo de Gestión de la USATI	Planilla control de asistencia diaria	Planilla control de asistencia diaria	Español	Físico	Físico	Disponible Archivo Gestión USATI
DOCUMENTOS DE ORIGEN CIUDADANO	Documento	Archivo de Gestión de la USATI	Derechos de petición y Tutelas	Oficio contentivo de la petición y soportes, oficio de traslado a otras entidades o dependencia competente, respuesta de trámite y/o de fondo, oficio de remisión a participación ciudadana, oficio de información de adminisión de la tutela y soportes, oficio de respuesta y soportes, oficio de comunicación de la decisión de tutela y soportes, documento de cumplimiento a lo ordenado en el título, documento de impugnación, trámite de	Español	Físico y/o Electronico	Tiff Sigedoc y/o físico	Disponible Archivo Gestión USATI
ESTUDIOS	Documento	Archivo de Gestión de la USATI	Estudios previos	Comunicaciones oficiales relacionadas con el estudio previo, comunicaciones oficiales solicitando cotizaciones, cotizaciones, Certificado de	Español	Físico y/o Electronico	PDF	Publicado en SECOP
INFORMES	Documento	Archivo de Gestión de la USATI	Informes de Gestión	Informes de gestión, anexo y comunicaciones oficiales relacionadas con el informe de gestión, informe de gestión documental GRE-81115-AX-18, anexos, consulta sobre gestión documental,	Español	Físico y/o Electronico	Tiff Sigedoc y/o físico	Disponible Archivo Gestión USATI
INVENTARIOS	Documento	Archivo de Gestión de la USATI	Inventario de eliminaciones documentales, Inventarios de transferencias documentales primarias	Formato único de inventario documental -GRE-81115-AX-04, copia control de visitas de gestión documental -GRE-81115-AX-09, acta de eliminación documental -GRE-81115-AX-13, acta de entrega de documentos al Fondo de Bienestar de la CGR -GRE-81115-AX-14, informe de eliminación documental -GRE-81115-AX-12, comunicaciones oficiales relacionadas con el inventario de eliminaciones documentales, o transferencias documentales primarias, reporte de errores en transferencias -GRE-81115-AX-10, acta final de transferencias documentales -GRE-81115-AX-11.	Español	Físico y/o Electronico	Tiff Sigedoc y/o físico	Disponible Archivo Gestión USATI
LIBRO RADICADOR DE COMUNICACIONES OFICIALES	Documento	Archivo de Gestión de la USATI	Libro radicador de comunicaciones oficiales	Libro radicador de comunicaciones oficiales	Español	Físico	Físico	Disponible Archivo Gestión USATI
NOVEDADES DE PERSONAL	Documento	Archivo de Gestión de la USATI	Novedades de Personal	Formato de permisos, permisos de ingreso a la institución, comunicaciones oficiales de: Horas extras solicitud, horas extras cumplidos, remitiendo evaluaciones, remitiendo concertaciones,	Español	Físico y/o Electronico	Tiff Sigedoc, PDF y/o Físico	Disponible Archivo Gestión USATI y en aplicativos institucionales
REGISTRO DE CONTROL DE SERVICIOS DE ARCHIVO	Documento	Archivo de Gestión de la USATI	Registro de control de consulta, Registro de control de préstamo, Registro de control de reprografía	Formato de solicitud y registro del servicio de: Consulta -GRE-81115-AX-16, Prestamo -GRE-81115-AX-15, Reprografía -GRE-81115-AX-17. Comunicaciones oficiales relacionadas con el	Español	Físico y/o Electronico	Tiff Sigedoc y/o físico	Disponible Archivo Gestión USATI

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS								Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB.	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
SISTEMA INTEGRADO DE GESTION Y CONTROL DE CALIDAD	Documento	Archivo de Gestión de la USATI	Acciones de mejora, Actas de circulo de mejoramiento, manuales de procedimientos, regiesgos institucional (solo para macroprocesos), plan de acción, plan de mejoramiento institucional.	Comunicación oficial remitiendo la acción de mejora, formato propuesta de mejora continua y actualización de documentos APP-80117-F-01, comunicaciones oficiales relacionadas con acciones de mejora, Actas de círculo de mejoramiento, anexos, comunicaciones oficiales relacionadas con actas de círculo de mejoramiento, Manuales de mejoramiento de Macroprocesos, procedimientos, instructivos, comunicaciones oficiales relacionadas con manuales de procedimientos, procedimientos e instructivos, Formato "Mapa de Riesgos Institucional" -DET-80117-AX-01, comunicaciones	Español	Físico y/o Electronico	PDF y/o físico	Disponible Archivo Gestión USATI y en aplicativos institucionales
SUPERVISIÓN CONTRATOS	Documento	Archivo de Gestión de la USATI, Página	Supervición contratos	Certificaciones, copia de actas e informes de supervisión y comunicaciones oficiales relacionadas con supervisión de contratos y sus anexos.	Español	Físico y/o Electronico	PDF y/o físico	Disponible Archivo Gestión USATI
ACCIÓN DE CUMPLIMIENTO	Documento	Documento Impreso	Demanda	Demanda donde la CGR es parte	Español	Fisico	Documento Texto	Oficina Juridica
ACCIÓN DE INCONSTITUCIONALIDAD	Documento	Documento Impreso	Demanda	Demanda donde la CGR es parte	Español	Fisico	Documento Texto	Oficina Juridica
ACCIONES POPULARES	Documento	Documento Impreso	Demanda	Demanda donde la CGR es parte	Español	Fisico	Documento Texto	Oficina Juridica
ACCIÓN DE REPETICIÓN	Documento	Documento Impreso	Demanda	Demanda donde la CGR es parte	Español	Fisico	Documento Texto	Oficina Juridica
ACTAS DE COMITÉ DE CONCILIACIÓN	Documento	Documento Impreso	Actas	Actas Comité	Español	Fisico	Documento Texto	Oficina Juridica
ANTECEDENTES DE TRÁMITES EXCEPCIONALES	Documento	Documento Impreso	Antecedentes	Antecedentes	Español	Fisico	Documento Texto	Oficina Juridica
CONCEPTOS JURÍDICOS	Documento	Documento Impreso (Digital	Conceptos	Conceptos	Español	Fisico	Documento Texto	Oficina Juridica
CONCILIACIONES PREJUDICIALES	Documento	Documento Impreso	Conciliaciones	Conciliaciones	Español	Fisico	Documento Texto	Oficina Juridica
CONTROL EXCEPCIONAL	Documento	Documento Impreso	Control	Control	Español	Fisico	Documento Texto	Oficina Juridica
EDICTOS	Documento	Documento Impreso	Edictos	Edcitos	Español	Fisico	Documento Texto	Oficina Juridica
AUTOS PROCESOS RESPONSABILIDAD FISCAL, PROCESOS ADMINISTRATIVOS SANCIONATORIOS FISCALES Y TRÁMITES EXCEPCIONALES	Documento impr	Documento Impreso	Autos	Autos	Español	Fisico	Documento Texto	Oficina Juridica
FALLOS PROCESOS RESPONSABILIDAD FISCAL	Documento	Documento Impreso	Fallos	Fallos	Español	Fisico	Documento Texto	Oficina Juridica
HOJA DE RUTA TRÁMITES	Documento	Documento Impreso	Hoja de Ruta	Hoja de Ruta	Español	Fisico	Documento Texto	Oficina Juridica
INFORMES DE AUDITORÍA EXTERNA	Documento	Documento Impreso	Informes	Informes	Español	Fisico	Documento Texto	Oficina Juridica
INFORMES DE CONTROL INTERNO	Documento	Documento Impreso	Informes	Informes	Español	Fisico	Documento Texto	Oficina Juridica
INFORMES DE PLANEACIÓN	Documento	Documento Impreso	Informes	Informes	Español	Fisico	Documento Texto	Oficina Juridica
INFORMES DIRECCIÓN FINANCIERA	Documento	Documento Digital	Informes	Informes	Español	Digital	Hoja Calculo	Oficina Juridica
INFORMES INTERNOS	Documento	Documento Digital	informes	Informes	Español	Digital	Hoja Calculo	Oficina Juridica
INFORMES MINISTERIO DEL INTERIOR Y JUSTICIA	Documento	Documento Impreso	Informes	Informes	Español	Fisico	Documento Texto	Oficina Juridica
INFORMES PROCURADURÍA GENERAL DE LA NACIÓN	Documento	Documento Impreso	Informes	Informes	Español	Fisico	Documento Texto	Oficina Juridica

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS								Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB.	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
SISTEMA INTEGRADO DE GESTION Y CONTROL DE CALIDAD	Documento	Archivo de Gestión de la USATI	Acciones de mejora, Actas de circulo de mejoramiento, manuales de procedimientos, regiesgos institucional (solo para macroprocesos), plan de acción, plan de mejoramiento institucional.	Comunicación oficial remitiendo la acción de mejora, formato propuesta de mejora continua y actualización de documentos APP-80117-F-01, comunicaciones oficiales relacionadas con acciones de mejora, Actas de círculo de mejoramiento, anexos, comunicaciones oficiales relacionadas con actas de círculo de mejoramiento, Manuales de mejoramiento de Macroprocesos, procedimientos, instructivos, comunicaciones oficiales relacionadas con manuales de procedimientos, procedimientos e instructivos, Formato "Mapa de Riesgos Institucional" -DET-80117-AX-01, comunicaciones	Español	Físico y/o Electronico	PDF y/o físico	Disponible Archivo Gestión USATI y en aplicativos institucionales
SUPERVISIÓN CONTRATOS	Documento	Archivo de Gestión de la USATI, Página	Supervición contratos	Certificaciones, copia de actas e informes de supervisión y comunicaciones oficiales relacionadas con supervisión de contratos y sus anexos.	Español	Físico y/o Electronico	PDF y/o físico	Disponible Archivo Gestión USATI
ACCIÓN DE CUMPLIMIENTO	Documento	Documento Impreso	Demanda	Demanda donde la CGR es parte	Español	Fisico	Documento Texto	Oficina Juridica
ACCIÓN DE INCONSTITUCIONALIDAD	Documento	Documento Impreso	Demanda	Demanda donde la CGR es parte	Español	Fisico	Documento Texto	Oficina Juridica
ACCIONES POPULARES	Documento	Documento Impreso	Demanda	Demanda donde la CGR es parte	Español	Fisico	Documento Texto	Oficina Juridica
ACCIÓN DE REPETICIÓN	Documento	Documento Impreso	Demanda	Demanda donde la CGR es parte	Español	Fisico	Documento Texto	Oficina Juridica
ACTAS DE COMITÉ DE CONCILIACIÓN	Documento	Documento Impreso	Actas	Actas Comité	Español	Fisico	Documento Texto	Oficina Juridica
ANTECEDENTES DE TRÁMITES EXCEPCIONALES	Documento	Documento Impreso	Antecedentes	Antecedentes	Español	Fisico	Documento Texto	Oficina Juridica
CONCEPTOS JURÍDICOS	Documento	Documento Impreso (Digital	Conceptos	Conceptos	Español	Fisico	Documento Texto	Oficina Juridica
CONCILIACIONES PREJUDICIALES	Documento	Documento Impreso	Conciliaciones	Conciliaciones	Español	Fisico	Documento Texto	Oficina Juridica
CONTROL EXCEPCIONAL	Documento	Documento Impreso	Control	Control	Español	Fisico	Documento Texto	Oficina Juridica
EDICTOS	Documento	Documento Impreso	Edictos	Edcitos	Español	Fisico	Documento Texto	Oficina Juridica
AUTOS PROCESOS RESPONSABILIDAD FISCAL, PROCESOS ADMINISTRATIVOS SANCIONATORIOS FISCALES Y TRÁMITES EXCEPCIONALES	Documento impr	Documento Impreso	Autos	Autos	Español	Fisico	Documento Texto	Oficina Juridica
FALLOS PROCESOS RESPONSABILIDAD FISCAL	Documento	Documento Impreso	Fallos	Fallos	Español	Fisico	Documento Texto	Oficina Juridica
HOJA DE RUTA TRÁMITES	Documento	Documento Impreso	Hoja de Ruta	Hoja de Ruta	Español	Fisico	Documento Texto	Oficina Juridica
INFORMES DE AUDITORÍA EXTERNA	Documento	Documento Impreso	Informes	Informes	Español	Fisico	Documento Texto	Oficina Juridica
INFORMES DE CONTROL INTERNO	Documento	Documento Impreso	Informes	Informes	Español	Fisico	Documento Texto	Oficina Juridica
INFORMES DE PLANEACIÓN	Documento	Documento Impreso	Informes	Informes	Español	Fisico	Documento Texto	Oficina Juridica
INFORMES DIRECCIÓN FINANCIERA	Documento	Documento Digital	Informes	Informes	Español	Digital	Hoja Calculo	Oficina Juridica
INFORMES INTERNOS	Documento	Documento Digital	informes	Informes	Español	Digital	Hoja Calculo	Oficina Juridica
INFORMES MINISTERIO DEL INTERIOR Y JUSTICIA	Documento	Documento Impreso	Informes	Informes	Español	Fisico	Documento Texto	Oficina Juridica
INFORMES PROCURADURÍA GENERAL DE LA NACIÓN	Documento	Documento Impreso	Informes	Informes	Español	Fisico	Documento Texto	Oficina Juridica

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS									Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE	
INFORMES SINOR	Document	Document o Digital	Informes	Informes	Español	Digital	Documento Texto	Pagina Web	
PROCESOS CIVILES	Document	Document o Impreso	Demanda	Demanda donde le CGR es parte	Español	Fisico	Documento Texto	Oficina Juridica	
PROCESOS CONTENCIOSOS ADMINISTRATIVOS	Document	Document o Impreso	Demanda	Demanda doncontenciosos la CGR es parte	Español	Fisico	Documento Texto	Oficina Juridica	
PROCESOS PENALES	Document	Document o Impreso	Demanda	Demanda donde le CGR es parte	Español	Fisico	Documento Texto	Oficina Juridica	
RESOLUCIONES ORDINARIAS DESPACHO DEL Gerente	Document	Document o Diigital	Resoluciones	Resoluciones	Español	Digital	Imagen	Oficina Juridica	
RESOLUCIONES ORDINARIAS OFICINA JURÍDICA	Document	Document o Digital	Resoluciones	Resoluciones	Español	Digital	Imagen	Oficina Juridica	
RESOLUCIONES ORGÁNICAS	Document	Document o Digitial	Resoluciones	Resoluciones	Español	Digital	Imagen	Pagina Web	
RESOLUCIONES REGLAMENTARIAS	Document	Document o Digitial	Resoluciones	Resoluciones	Español	Digital	Imagen	Pagina Web	
COLECCIÓN MATERIAL AUDIOVISUAL	Video	Video	Videos informativos institucionales	Videos de carácter institucional que registran eventos y la gestipon de la entidad en temas relacionados con su quehacer misional	Español	Digital	Digital	Página Web	
BOLETINES DE PRENSA	Docu	Documento	Boletín de prensa	Documento electrónico presenta de manera noticiosa la gestión de la entidad en temas específicos y la cual tiene como destino los medios	Español	Digital	Digital	Página Web	
PUBLICACIONES INSTITUCIONALES	Docu ment o impr	Libros, revistas, informes, folletos	Publicaciones institucionales	Documento de carácter técnico que recoge los resultados de gestión, estudios o artículos afines al quehacer institucional.	Español	impreso y/ o digital	impreso y/ o digital	página web , Oficina de Comunicaciones, en caso de que la publicación haya sido impresa	
REGISTRO MEDIOS DE COMUNICACIÓN	Docu	Documento	Registro de prensa	Documento electrónico mencionado en la página web de la entidad para ilustrar cómo los medios de comunicación registran las noticias emitidas por la	Español	Digital	Digital	Página Web	
PLAN ANUAL DE COMUNICACIONES	Docu	Documento	Plan anual de comunicaciones	Dcumento electrónico que evidencia las estrategias y acciones que emprenderá la entidad en temas de comunicación organizacional	Español	Digital	Digital	Página Web	
DISCURSOS Gerente GENERAL DE LA REPÚBLICA	Docu	Documento	Discursos Gerente General de la República	Intervenciones del Gerente General en eventos públicos, donde se da a conocer la versión oficial de la entidad siobre un tema respectivo	Español	Digital	Digital	Página Web	
ACTAS COMITÉ DE ÉTICA		Documento	Actas	Desarrollo de los Planes de Acción a seguir sobre el tema de ética.	Español	Físico y digital	Word	Disponible	
EXPEDIENTES DISCIPLINARIOS		Expediente (Proceso Disciplinario con auto de formulación de cargos, finalizado, archivo)	Queja ó antecedente, Indagación Preliminar, Investigación.	Procesos disciplinarios adelantados contra funcionarios ó exfuncionarios de la entidad.	Español	Físico y digital	Word, pdf	Disponible	
SUSTANCIACIONES (Inhibitorios)		Documento	Queja ó antecedente, Auto inhibitorio	Excepción a la apertura de un proceso disciplinario	Español	Físico y digital	Word, pdf	Disponible	
DERECHOS DE PETICIÓN		Documento	Derecho de petición y repuesta.	Solicitud de información de procesos disciplinarios contra funcionarios y/o exfuncionarios.	Español	Físico y digital	Word, pdf	Disponible	
TUTELAS		Documento	Tutela, respuesta	Solicitud de respuesta y complementación de repuesta a derechos de petición.	Español	Físico y digital	Word, pdf	Disponible	
ACTAS DE COMITÉ DE COORDINACIÓN DEL SISTEMA DE CONTROL INTERNO - CCSCI	Bases de Datos	Actas de comités CCSCI una vez firmadas	ACTAS DE COMITÉ DE COORDINACIÓN DEL SISTEMA DE CONTROL INTERNO	Pautas para la determinación, implementación, adaptación y mejoramiento permanente del Sistema de Control Interno.	Español	Físico	Papel	Archivo de Gestión de la Oficina de Control Interno Archivo Centralizado y archivo central de la CGR	
ACTAS DE COMITÉ TÉCNICO DE LA OFICINA DE CONTROL INTERNO	Bases de Datos	Actas de comité técnico de la OCI	ACTAS DE COMITÉ TÉCNICO DE LA OCI	Planeación, ejecución , validación de hllazgos, entre otras.	Español	Físico	Papel	Archivo de Gestión de la Oficina de Control Interno. Archivo Centralizado y archivo central de la CGR.	
ACTUACIONES DE SEGUIMIENTO, ACOMPAÑAMIENTO Y ASESORÍA	Bases de Datos	Informes	Actuaciones de seguimiento, acompañamiento y asesoría	Actuaciones en tiempo real	Español	Físico	Papel	Archivo de Gestión de la Oficina de Control Interno. Archivo Centralizado y archivo central de la CGR.	
REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS									Versión 1.0

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS								Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
AUDITORÍA INTERNA	Bases de datos	Informe de auditoria interna	Auditoria Interna	Auditorias	Español	Físico	Papel	Archivo de Gestión de la Oficina de Control Interno. Archivo Centralizado y archivo central de la CGR.
CERTIFICACIONES SEMESTRALES SOBRE EL CUMPLIMIENTO DE LAS OBLIGACIONES DE LAINSTITUTO NACIONAL DE MUSEOSFRENTE AL SISTEMA ÚNICO DE GESTIÓN E INFORMACIÓN LITIGIOSA DEL ESTADO	Bases de Datos	Certificación de la Oficina de la Oficina de Control Interno	Actuación de Seguimiento	Emitir certificación del trámite procesal de la Defensa Judicial de la CGR	Español	Físico	Papel	Archivo de Gestión de la Oficina de Control Interno. Archivo Centralizado y archivo central de la CGR.
INFORMES DE AUDITORÍA INTERNA	Bases de Datos	Informes de auditoria interna.	Auditoria Interna	Informes	Español	Físico	Papel	Archivo de Gestión de la Oficina de Control Interno. Archivo Centralizado y archivo central de la CGR.
INFORMES DE CONTROL INTERNO CONTABLE	Bases de Datos	Informe presentados a la Contaduría General de la	Auditoria Proceso contable	Informes Publicado WEB de la Contaduría	Español	Físico	Papel	Archivo de Gestión de la Oficina de Control Interno. Archivo Centralizado y archivo central de la CGR. En la WEB de la CGR.
INFORMES EJECUTIVOS ANUALES DE CONTROL INTERNO	Base de Datos	Informe presentado al DAFP	Actuación de Seguimiento	Informes	Español	Físico	Papel	Archivo de Gestión de la Oficina de Control Interno. Archivo Centralizado y archivo central de la CGR. En la WEB de la CGR.
INFORMES PORMENORIZADOS DEL ESTADO DE CONTROL INTERNO EN LA GerenteÍA GENERAL DE LA REPÚBLICA	Base de Datos	Informe presentado a la ciudadanía	Actuación de Seguimiento	Informes publicado WEB de la CGR	Español	Físico	Papel	Archivo de Gestión de la Oficina de Control Interno. WEB de la CGR
INFORMES RENDIDOS POR DEPENDENCIAS DE LA GerenteÍA GENERAL DE LA REPÚBLICA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
INFORMES SEMESTRALES SOBRE ATENCIÓN DE QUEJAS, SUGERENCIAS Y RECLAMOS DE LA CIUDADANÍA RELACIONADOS CON LA MISIÓN DE LA CGR	Base de Datos	Informe de seguimiento a los Derechos de petición y	Actuación de Seguimiento	Informes	Español	Físico	Papel	Archivo de Gestión de la Oficina de Control Interno. Archivo Centralizado y archivo central de la CGR.
INFORMES TRIMESTRALES SOBRE CUMPLIMIENTO DE MEDIDAS DE AUSTERIDAD Y EFICIENCIA EN EL GASTO PÚBLICO EN LA CGR	Bases de Datos	Informes	Actuación de Seguimiento	Informes	Español	Físico	Papel	Archivo de Gestión de la Oficina de Control Interno. Archivo Centralizado y archivo central de la CGR.
PLAN DE AUDITORIA INTERNA (PAI)	Base de Datos	Acta de comité de coordinación del Sistema de control interno	Programación de auditorias anuales	Plan de Auditoria Interna Aprobado	Español	Físico	Papel	Archivo de Gestión de la Oficina de Control Interno. Archivo Centralizado y archivo central de la CGR.
REPORTES SE SEGUIMIENTO A LAS ESTRATÉGIAS DEL PLAN ANTICORRUPCIÓN Y DE ATENCIÓN AL CIUDADANO EN LA GerenteÍA GENERAL DE LA REPÚBLICA	Base de Datos	Informe seguimiento cuatrimestral	Actuación de Seguimiento	Informe	Español	Físico	Papel	Archivo de Gestión de la Oficina de Control Interno.
PROCESO VIA GUBERNATIVA - APELACIÓN TARIFA FISCAL	NO	SI	Recursos de apelación a la tarifa de control fiscal	Decisión del recurso de apelación al acto que establece la tarifa de control fiscal.	Español	Físico	Documento de texto	Original disponible en la Oficina de Planeación
CONVENIOS CON PROCURADURÍA FISCALIA	NO	SI	Convenio tripartito	Convenio de cooperación interinstitucional	Español	Físico	Documento de texto	Despacho ViceGerente
ACTAS DE COMITÉ TÉCNICO	NO	SI	Actas de Comité Tècnico Oficina de Planeaciòn	Temas tratados en el comité técnico de la oficina de planeación	Español	Físico	Documento de Texto	Disponible en la Oficina de Planeación.

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS									Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
ACTAS DE SEGUIMIENTO Y EVALUACIÓN ESTRATÉGICA DE INFORMACIÓN	NO EXISTE. EN PROCESO DE ACTUALIZACIÓN TABLA DE RETENCIÓN DOCUMENTAL							
INFORMES AL CONGRESO SOBRE EL CUMPLIMIENTO DE LAS FUNCIONES DEL Gerente GENERAL	SI	SI	Informe de Gestión al Congreso y al Presidente de la República	Informe sobre el cumplimiento de las funciones del Gerente General de la Repùblica	Español	Digital	Documento de Texto	Disponible en Web
INFORMES BENEFICIOS A SUJETOS DE CONTROL FISCAL	SI	SI	Incluido en el Informe de Gestión al Congreso	Beneficios generados del ejercicio del control fiscal	Español	Digital	Documento de Texto	Físico y Web
INFORMES DE COSTOS - SISTEMA DE COSTEO	NO	SI	Informes de Costos - Sistema de Costeo	Consolidación del registro de los costos de operación de la Gerenteía General de la República	Español	Digital	Documento de Texto	Digital
INFORMES DE EVALUACIÓN DE LA GESTIÓN PÚBLICA	NO EXISTE. EN PROCESO DE ACTUALIZACIÓN TABLA DE RETENCIÓN DOCUMENTAL							
INFORMES DE EVALUACIÓN Y CONCEPTUALIZACIÓN SISTEMA DE CONTROL INTERNO	SI	SI	Informe de resultados Evaluación de la Calidad y Eficiencia del Control Fiscal Interno de las entidades públicas	Informe de resultados Evaluación de la Calidad y Eficiencia del Control Fiscal Interno de las entidades públicas	Español	Digital	Documento de Texto	Digital
INFORMES DE GESTIÓN	NO EXISTE. EN PROCESO DE ACTUALIZACIÓN TABLA DE RETENCIÓN DOCUMENTAL							
INFORMES DE GESTIÓN DE LA ENTIDAD	NO EXISTE. EN PROCESO DE ACTUALIZACIÓN TABLA DE RETENCIÓN DOCUMENTAL							
INFORMES PLANES DE MEJORAMIENTO SUJETOS DE CONTROL	NO EXISTE. EN PROCESO DE ACTUALIZACIÓN TABLA DE RETENCIÓN DOCUMENTAL							
INFORMES SISTEMA INTEGRADO DE RIESGOS INSTITUCIONALES - SIRI	NO EXISTE. EN PROCESO DE ACTUALIZACIÓN TABLA DE RETENCIÓN DOCUMENTAL							
METODOLOGÍA Y PROCEDIMIENTO DE CONTROL FISCAL	SI	SI	Guía de Auditoría de la Gerenteía General de la República	Procedimiento para ejercer el proceso auditor.	Español	Digital	Documento de Texto	Web
AJUSTE AL PLAN GENERAL DE AUDITORÍA	SI	SI	Plan de Vigilancia y Control Fiscal	Relación de las entidades y asuntos a auditar en una vigencia	Español	Digital	Hoja Electrónica	Web
LINEAMIENTOS Y PROGRAMACIÓN INICIAL DEL PLAN GENERAL DE AUDITORÍA	SI	SI	Lineamientos para Elaboración y Ejecución del Plan de Vigilancia y Control Fiscal	Lineamientos para Elaboración y Ejecución del Plan de Vigilancia y Control Fiscal.	Español	Digital	Documento de Texto	Web
SEGUIMIENTO AL PLAN GENERAL DE AUDITORÍA	NO	NO	Seguimiento al Plan de Vigilancia y Control Fiscal	Registros sobre el monitoreo al avance de las auditorias programadas	Español	Digital	Documento de Texto.	Disponible en la Oficina de Planeación.
PLAN NACIONAL DE AUDITORÍA	NO	SI	Plan Nacional de Auditoría	Relaciòn de las auditorías programadas por laINSTITUTO NACIONAL DE MUSEOSy las Gerenteías Territoriales	Español	Digital	Hoja Electrónica	Disponible en la Oficina de Planeación.
PROGRAMACIÓN PRESUPUESTAL	NO	SI	Anteproyecto de Presupuesto y marco de gasto de mediano plazo	Justificación y soportes programación presupuestal de la vigencia	Español	Físico	Documento de Texto.	Disponible en la Oficina de Planeación.
PROYECTOS DE INVERSIÓN	NO	SI	Proyectos de Inversión	Información general básica de los proyectos de inversión.	Español	Digital	Sistema de información de proyectos de inversión (SPI)	En Web Departamento Nacional de Planeación
PROYECTOS DE RESOLUCIONES DE RENDICIÓN DE CUENTAS E INFORMES SUJETOS DE CONTROL FISCAL	NO EXISTE. EN PROCESO DE ACTUALIZACIÓN TABLA DE RETENCIÓN DOCUMENTAL							
PROYECTOS DE RESOLUCIONES DE SECTORIZACIÓN Y CARACTERIZACIÓN SUJETOS DE CONTROL	SI	SI	Resoluciones de Sectorización y Categorización de Sujetos de Control.	Relación de los sujetos de control por cada Gerenteía Delegada Sectorial.	Español	Físico y Digital	Documento de Texto	Web y Oficina de Planeación
RENDICIÓN DE LA CUENTA DE LAINSTITUTO NACIONAL DE MUSEOSA LA AUDITORÍA GENERAL DE LA REPÚBLICA	NO	NO	Rendición de la Cuenta de laINSTITUTO NACIONAL DE MUSEOSa la Auditoría General de la República	Información sobre la gestión de la Gerenteía General de la República	Español	Digital	Documento de Texto, Hoja de Cálculo	NO
SOLICITUDES Y REQUERIMIENTOS DE LA AUDITORÍA GENERAL DE LA REPÚBLICA	NO	NO	Solicitudes y Requerimientos de la Auditoría General de la República	Información sobre la gestión de la Gerenteía General de la República	Español	Digital	Documento de Texto, Hoja de Cálculo	NO

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS									Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
REVISIÓN TÉCNICA DE CONVENIOS	No aplica	No aplica	Revisión Técnica de Convenios	Revisión Técnica de Convenios	Español	Físico	Documento de Texto	NO
SISTEMA DE RENDICIÓN ELECTRÓNICA DE LA CUENTA E INFORMES - SIRECI	NO	SI	Sistema de Rendición Electrónica de la Cuenta e Informes - SIRECI	Información sobre la gestión de las entidades Vigiladas por la Gerenteía General de la República	Español	Digital	Documento de Texto, Hoja de Cálculo	NO
SISTEMA INTEGRADO DE GESTIÓN Y CONTROL DE CALIDAD - SIGCC	NO	No aplica, porque la documentación está en proceso de revisión para su actualización	Sistema Integrado de Gestión y Control de Calidad - SIGCC	Documentos del Sistema Integrado de Gestión y Control de Calidad - SIGCC	Español	Digital	Documento de Texto	No aplica, Porque la documentación esta en proceso de revisión para su actualización
ACCIONES DE MEJORA	NO	No aplica	Acciones de Mejora	Propuesta de creación, actualización y eliminación de docuemtnos del Sistema Integrado de Gestión y Control de Calidad - SIGCC	Español	Digital	Documento de Texto	No aplica, Porque se trata de propuesta de creación, actualización y eliminación de documentos del Sistema Integrado de Gestión y Control de Calidad
ACTAS DE CÍRCULO DE MEJORAMIENTO (Subserie Documental Común en la CGR)	NO EXISTE. EN PROCESO DE ACTUALIZACIÓN TABLA DE RETENCIÓN DOCUMENTAL							
MANUALES DE PROCEDIMIENTOS	NO	No aplica, porque la documentación está en	Manuales de Procedimientos	Documentos del Sistema Integrado de Gestión y Control de Calidad - SIGCC	Español	Digital	Documento de Texto.	No aplica, Porque la documentación esta en proceso de revisión para su actualización
MAPA DE RIESGOS Y PLAN DE MANEJO DE RIESGOS INSTITUCIONAL	NO	No aplica, porque la metodología de administración de riesgos está en proceso de revisión para su actualización	Mapa de Riesgos y Plan de Manejo de Riesgo Institucional.	Mapa de Riesgos y Plan de Manejo de Riesgo Institucional.	Español	Digital	Documento de Texto.	No aplica, porque la metodología de administración de riesgos esta en proceso de revisión para su actualización
PLAN ESTRATÉGICO Y PLAN DE ACCIÓN	SI	SI	Plan Estrátegico y Plan de Acción.	Plan Estrátegico y Plan de Acción.	Español	Digital	Documento de Texto.	Web
PLAN DE MEJORAMIENTO INSTITUCIONAL	NO	SI	Plan de Mejoramiento Institucional.	Plan de Mejoramiento Institucional.	Español	Digital	Hoja Electrónica	Disponible en la Oficina de Planeación.
REVISIÓN DEL SIGCC	NO EXISTE. EN PROCESO DE ACTUALIZACIÓN TABLA DE RETENCIÓN DOCUMENTAL							
ASISTENCIA TÉCNICA DEL SISTEMA NACIONAL DE CONTROL FISCAL - SINACOF	NO	SI	Asistencia Técnica del Sistema Nacional de Control Fiscal-SINACOF	Registros sobre la asistencia técnica brindada por la Gerenteía General a las Gerenteías Territoriales.	Español	Físico y Digital	Documento de Texto.	Disponible en la Oficina de Planeación.
SEMINARIOS Y TALLERES DEL SISTEMA NACIONAL DE CONTROL FISCAL - SINACOF	NO	SI	Seminarios y Talleres del Sistema Nacional de Control Fiscal - SINACOF	Registros sobre la realización de seminarios y talleres.	Español	Físico	Documento de Texto.	Disponible en la Oficina de Planeación.
ANTECEDENTES DE TARIFA DE CONTROL FISCAL	NO	SI	Antecedentes de Tarifa de Control Fiscal	Documentos soporte para la liquidación de la tarifa de control fiscal.	Español	Físico	Documento de Texto.	Disponible en la Oficina de Planeación.
RESOLUCIONES NOTIFICADAS DE TARIFA DE CONTROL FISCAL	NO	SI	Resoluciones Notificadas de Tarifa de Control Fiscal.	Resoluciones Notificadas de Tarifa de Control Fiscal.	Español	Físico y Digital	Documento de Texto.	Disponible en la Oficina de Planeación.
RECURSOS DE TARIFA DE CONTROL FISCAL	NO	SI	Recursos de Tarifa de Control Fiscal	Trámite de los recursos interpuestos contra las resoluciones que fijan la tarifa de control fiscal.	Español	Físico	Documento de Texto.	Disponible en la Oficina de Planeación.
SOLICITUDES DE CONTROL FISCAL	NO	SI	Solicitude de Tarifa de Control Fiscal	Otros requerimientos relacionados con la liquidación de la tarifa de control fiscal.	Español	Físico	Documento de Texto.	Disponible en la Oficina de Planeación.
ACTAS DE COMITÉ DE OPERACIONES DEL SICE	NO	SI	Actas de comité de operaciones del SICE	Contiene actas de reuniones de operación del SICE	Español	Físico	Documento de Texto Carta-oficio	Archivo de Gestión de la Oficina de Sistemas e Informática (5 años) y 10 años en Archivo Central de la CGR
ACTAS DE COMITÉ TÉCNICO	NO	SI	Actas de Comité Técnico	Contiene actas de reuniones de operación del SICE	Español	Físico	Documento de Texto Carta-oficio	Archivo de Gestión de la Oficina de Sistemas e Informática (5 años) y 10 años en Archivo Central de la CGR

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS								Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
AUTORIZACIÓN DE BAJA DE EQUIPOS	NO	SI	Autorización baja de equipos de cómputo	Solicitud, aprobación y/o negación de la baja	Español	Físico	Documento de Texto Carta-oficio	Archivo de Gestión de la Oficina de Sistemas e Informática (5 años)
DESARROLLO Y MANTENIMIENTO DE SOFTWARE	NO	SI	Desarrollo y mantenimiento de software	Se encuentra aqui toda la información técnica de cada aplicativo desarrollado por la Entidad o contratado su desarrollo	Español	Digital	PDF, Word	Para funcionarios autorizados en \\SCFS01\Informacion OSEI\DOCUMENTACION_APLICACIONES
MANUALES TÉCNICOS	NO	SI	Manuales técnicos del sistema.	Manuales técnicos de cada uno de los sistemas	Español	Digital	PDF, Word	Solo para funcionarios autorizados
MANUALES DEL USUARIO	NO	SI	Manuales de usuario del sistema.	Manuales de usuario del aplicativo	Español	Digital	PDF, Excel, Word	Solo para funcionarios autorizados
MANUALES DEL SISTEMA	NO	SI	Manuales técnicos del sistema.	Manuales con las características técnicas de cada uno de los sistemas de información.	Español	Digital	PDF, Word	Solo para funcionarios autorizados
REQUERIMIENTOS A MESA DE AYUDA	SI	SI	Requerimientos a mesa de ayuda	Requerimientos o reporte de incidencias relacionadas con TI	Español	Físico, electrónico	Documento de texto, hoja de cálculo, documento PDF, reporte aplicativo	Archivo de Gestión de la Oficina de Sistemas e Informática Aplicativo GLPI
SISTEMA DE INFORMACIÓN PARA LA VIGILANCIA DE LA CONTRAATACIÓN ESTATAL								
CONSULTA ENTIDADES	SI	SI	Respuestas	Solicitudes hechas por entidades	Español	Físico	Documento de Texto Carta	SI
CONSULTA ENTES DE CONTROL	SI	SI	Respuestas	Solicitudes hechas por entes de control	Español	Físico	Documento de Texto Carta	SI
CONSULTA GRUPO DE CALIDAD	SI	SI	Consultas	Solicitud respuesta	Español	Físico	Documento de Texto Carta y Oficio	SI
CONSULTA GRUPO DE APOYO AL CONTROL FISCAL	SI	SI	Consultas	Solicitud respuesta	Español	Físico	Documento de Texto Carta y Oficio	SI
CONSULTA PROVEEDORES	SI	SI	Consultas de proveedores	Solicitud respuesta	Español	Físico	Documento de Texto Carta y Oficio	SI
DOCUMENTOS DE CAPACITACIÓN	SI	SI	Documentos de capacitación	Solicitudes capacitación	Español	Físico	Documento de Texto Carta y Oficio	SI
DOCUMENTOS CUBS E INTEROPERATIVIDAD DEL SISTEMA	SI	SI	Documentos CUBS e interoperatividad del sistema	Códigos de identificación.	Español	Físico	Documento de Texto Carta y Oficio	SI
NORMATIVIDAD SICE	SI	SI	Resoluciones	Normatividad SICE	Español	Físico	Documento de Texto Carta y Oficio	SI
INFORMES DE RENDICION DE CUENTAS A LA AUDITORÍA GENERAL DE LA REPÚBLICA - FORMATO 24 - SIREL	SI	SI	Informes Oficina de Sistemas e Informática	Formato 24, informes de rendición de cuentas de las auditorías de ley realizada por la AGR	Español	Medio magnético, base de datos de la AGR	Suite de Microsoft y ODF	Si, una vez haya sido publicado por la AGR
PROCESOS DE SELECCIÓN PARA CAPACITACION INTERNACIONAL	Archivo de Gesti	Documento físico o magnético	Proceso de selección para capacitación internacional	Invitaciones, designación de participantes.	Español	Físico y magnético	Documento de texto, correo electrónico	Disponible en Archivo de Gestión de la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional
PROCESOS DE COOPERACION CON ENTIDADES INTERNACIONALES	Archivo de Gesti	Documento físico o magnético	Procesos de Cooperación con entidades internacionales	Comunicaciones oficiales	Español y otros	Físico y magnético	Documento de texto, correo electrónico	Disponible en Archivo de Gestión de la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional
ACTAS DE COMITE INSTITUCIONAL DE CAPACITACION	Archivo de Gesti	Documento	Actas del Comité Institucional de Capacitación	Actas y soportes	Español	Físico	Documento de texto	Disponible en Archivo de Gestión de la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS								Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
ACTAS DEL CONSEJO ACADÉMICO	Archivo de Gestión	Documento	Actas del Consejo Académico	Actas y soportes	Español	Físico	Documento de texto	Disponible en Archivo de Gestión de la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional
COMISIONES	Archivo de Gestión	Documento	Comisiones	Solicitud, soportes, Resolución de comisión, convenio de contraprestación, garantías, informe de comision, seguimiento obligaciones, acta de liquidación, acuerdos de pago.	Español	Físico	Documento de texto	Disponible en Archivo de Gestión de la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional
AVALES	Archivo de Gestión	Documento	Avales	Solicitud, soportes, aval.	Español y otros	Físico	Documento de texto	Disponible en Archivo de Gestión de la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional
COMISIONES DE ESTUDIOS AL INTERIOR DEL PAIS POR FUNCIONARIO	Archivo de Gestión	Documento	Comisiones de estudios al interior del país por funcionario	Solicitud, soportes, Resolución de comisión, convenio de contraprestación, garantías, informe de comision, seguimiento obligaciones, acta de liquidación, acuerdos de pago.	Español	Físico	Documento de texto	Disponible en Archivo de Gestión de la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional
COMISIONES DE ESTUDIOS EN EL EXTERIOR POR FUNCIONARIO	Archivo de Gestión	Documento	Comisiones de estudios al exterior por funcionario	Solicitud, soportes, Resolución de comisión, convenio de contraprestación, garantías, informe de comision, seguimiento obligaciones, acta de liquidación, acuerdos de pago.	Español y otros	Físico	Documento de texto	Disponible en Archivo de Gestión de la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional
COMISIONES DE SERVICIOS AL INTERIOR DEL PAIS	Archivo de Gestión	Documento	Comisiones de estudios al interior por funcionario	Solicitud, soportes, fotocopia Resolución de comisión, informe de comisión, cumplido de comisión.	Español y otros	Físico	Documento de texto	Disponible en Archivo de Gestión de la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional
COMISIONES DE SERVICIOS EN EL EXTERIOR	Archivo de Gestión	Documento	Comisiones de servicios al exterior	Solicitud, soportes, Resolución de comisión, informe de comisión, cumplido de comisión.	Español y otros	Físico	Documento de texto	Disponible en Archivo de Gestión de la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional
COMISIONES PARA ATENDER INVITACIÓN	Archivo de Gestión	Documento	Comisiones para atender invitación	Solicitud, soportes, Resolución de comisión, informe de comisión, cumplido de comisión.	Español y otros	Físico	Documento de texto	Disponible en Archivo de Gestión de la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional
SOLICITUDES DE COMISIONES NO APROBADAS	Archivo de Gestión	Documento	Solicitudes de comisión no aprobadas	Solicitud, soportes, comunicaciones oficiales.	Español y otros	Físico	Documento de texto	Disponible en Archivo de Gestión de la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional
CONVENIOS DE COOPERACION INTERNACIONAL	Archivo de Gestión	Documento	Convenios de Cooperación Internacional	Convenio, estudios y documentos previos, antecedentes, seguimiento, acta de liquidación, actas de cooridnación.	Español y otros	Físico	Documento de texto	Disponible en Archivo de Gestión de la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional
CONVENIOS DE COOPERACION NACIONAL	Archivo de Gestión	Documento	Convenios de Cooperación Nacional	Convenio, estudios y documentos previos, antecedentes, seguimiento, acta de liquidación, actas de cooridnación.	Español	Físico	Documento de texto	Disponible en Archivo de Gestión de la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional
PASANTIAS NO REMUNERADAS	Archivo de Gestión	Documento	Pasantías no remuneradas	Convenio, estudios y documentos previos, antecedentes, seguimiento, acta de liquidación, actas de cooridnación.	Español	Físico	Documento de texto	Disponible en Archivo de Gestión de la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional
DEREHOS DE PETICION	Archivos de Gestión	Documento	Derechos de Petición	Respuesta a solicitud	Español	Físico	Documento de texto	Disponible en Archivo de Gestión de la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional
HISTORIAS ACADÉMICAS DE DOCENTES Y/O INVESTIGADORES	Si	Si	Hojas de vida docentes	Historias académicas de docentes y/o investigadores	Español	Físico	Word	Disponible en Archivo de Gestión de la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS								Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
INFORMES DE AUDITORIA EXTERNA	Si	Si	Informes de auditoria externa	Informe de Auditoría Externa Comunicaciones oficiales relacionadas con el informe de auditoría externa	Español	Físico	Excel	Disponible en Archivo de Gestión de la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional
INFORMES DE GESTIÓN	Archivo de Gestión	Documento	Informe de Gestión	Informe de Gestión.	Español	Físico	Documento de texto	Disponible en Archivo de Gestión de la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional
PROTOCOLOS DE INVESTIGACIÓN			Protocolos de investigación	Proyectos de investigación realizados y desarrollados por serviodres publicos de la C.G.R. y protocolos para el desarrollo de la tarea investigativa	Español, Ingles,	Fisico, Magnetico		Disponible en Archivo de Gestión de la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional
PROYECTOS DE INVESTIGACIÓN			Proyectos de investigación	Proyectos de investigación realizados y desarrollados por serviodres publicos de la C.G.R. Inscritos y reconosidos por El Departamento Administrativo de Ciencia , tecnologuia e	Español, Ingles,	Magnetico, Digiital, Fisico, web	Validos toodos es muy variado, PDF,	http://190.242.114.26:8080/gruplac/. http://campus.Gerenteia.gov.co:8080 /investigacion
DIAGNÓSTICO DE NECESIDADES DE CAPACITACIÓN	Archivo de Gestión	Documento	Diagnóstico de necesidades de Capacitación	Instrumento diagnóstico, solicitudes de capacitación, consolidado diagnóstico.	Español	Físico	Documento de texto	Disponible en Archivo de Gestión de la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional
PLAN DE ACCIÓN	Archivo de Gestión	Documento físico y magnético	Plan de Acción	Plan de Acción.	Español	Físico	Documento de texto Magnético en PDF	Disponibleen Archivo de Gestión de la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional y en www.Gerenteia.gov.co
PLAN GENERAL DE CAPACITACIÓN	Archivo de Gestión www	Documento físico y magnético	Plan General de Capacitación	Plan General de Capacitación.	Español	Físico	Documento de texto Magnético en PDF	Disponible en Archivo de Gestión de la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional, www.Gerenteia.gov.co campus virtual
PROGRAMA ANUAL DE CAPACITACIÓN	Archivo de Gestión www	Documento físico y magnético	Programa Anual de Capacitación	Programa Anual de Capacitación.	Español	Físico	Documento de texto Magnético en PDF	Disponible en Archivo de Gestión de la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional, www.Gerenteia.gov.co campus virtual
PROCESO DE SELECCIÓN CRÉDITO EDUCATIVO CON CONTRAPRESTACIÓN DE SERVICIOS	Archivo de Gestión	Documento	Proceso de Selección Crédito Educativo con Contraprestación de Servicios	Convocatoria; listados de admitidos y no admitidos, comunicaciones relacionadas con el proceso de selección de créditos	Español	Físico	Documento de Texto	Disponible en Archivo de Gestión de la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional
CREDITOS EDUCATIVOS CON CONTRAPRESTACIÓN DE SERVICIOS	Archivo de Gestión	Documento	Créditos Educativos con Contraprestación de Servicios	Solicitudes aprobadas con soportes, Convenios, comunicaciones relacionadas con el credito educativo	Español	Físico	Documento de Texto	Disponible en Archivo de Gestión de la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional
SOLICITUDES NO APROBADAS DE CREDITOS EDUCATIVOS	Archivo de Gestión	Documento	Solicitudes no Aprobadas de Créditos Educativos	Solicitudes no admitidas, comunicaciones oficiales relacionadas con las mismas.	Español	Físico	Documento de Texto	Disponible en Archivo de Gestión de la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional
ACTIVIDADES Y EVENTOS DE CAPACITACION COMPLEMENTARIOS	Archivo de Gestión	Documento	Informe Final de Cursos Presenciales	Informes de curso	Español	FISICO	Documento en Excel	Disponible en Archivo de Gestión de la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional
DISEÑO DE CURSOS Y MATERIAL DIDÁCTICO	Archivo de Gestión	Documento	Diseño de cursos y material didáctico	Comunicaciones oficiales relacionadas con el diseño de cursos y material didáctico	Español	Papel y electrónica	Word, PDF, multimedia	Disponible en Archivo de Gestión de la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS **Versión 1.0**

CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
INFORME FINAL DE CURSOS PRESENCIALES	Archivo de Gestión	Documento	Informe Final de Cursos Presenciales	Convocatoria, inscripciones, contenidos, participantes, asistencia, libreta de calificaciones, evaluaciónes, acta final, Comunicaciones oficiales relacionadas con el informe final de cursos presenciales	Español	Papel y electrónica	Word	Disponible en Archivo de Gestión de la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional
INFORME FINAL DE CURSOS VIRTUALES	Archivo de Gestión	Documento	Informes Final de Cursos Virtuales	Convocatoria, inscripciones, contenidos, participantes, asistencia, libreta de calificaciones, evaluaciónes, acta final, Comunicaciones oficiales relacionadas con el informe final de cursos presenciales	Español	Papel y electrónica	Word	Disponible en Archivo de Gestión de la Oficina de Capacitación, Producción de Tecnología y Cooperación Técnica Internacional
CONSULTAS DE INFORMACIÓN DE OTRAS AUTORIDADES DE CONTROL, INSPECCIÓN Y VIGILANCIA	NO	SI	Consultas	Respuestas y conceptos a otras entidades.	Español	Medio Físico	Documentos de texto y/o hojas de cálculo	Disponible en Archivo de Gestión de la Gerenteía Delegada para Economía y Finanzas Públicas
CERTIFICACIONES SOBRE INGRESOS CORRIENTES LIBRE DESTINACIÓN	SI	SI	Certificados de Ingresos Corrientes	Certificacion de ingresos corrientes de libre destinación y su relacion con los gastos de funcionamiento	Español	Medio magnético	Documentos PDF	Publicada en: http://www.Gerenteia.gov.co/web/guest/certificados-ley-617
DEREHOS DE PETICIÓN	NO	SI	Respuesta a derechos de petición	Respuestas a solicitudes de la ciudadania o entidades	Español	Medio Físico	Documentos de texto y/o hojas de cálculo	Disponible en Archivo de Gestión de la Gerenteía Delegada para Economía y Finanzas Públicas
TUTELAS	NO	SI	Respuesta a tutelas	Respuestas a solicitudes de la ciudadania o entidades	Español	Medio Físico	Documentos de texto y/o hojas de cálculo	Disponible en Archivo de Gestión de la Gerenteía Delegada para Economía y Finanzas Públicas
PRORROGAS	NO	SI	Respuesta a prorrogas	Respuestas y solicitudes de prorroga para envío de información	Español	Medio Físico	Documentos de texto	Disponible en Archivo de Gestión de la Gerenteía Delegada para Economía y Finanzas Públicas
SOLICITUDES SOBRE DEUDA PUBLICA NACIONAL Y TERRITORIAL	NO	SI	Respuesta a solicitudes de información	Respuestas a solicitudes de la ciudadania o entidades	Español	Medio Físico	Documentos de texto	Disponible en Archivo de Gestión de la Gerenteía Delegada para Economía y Finanzas Públicas
INFORME DE AUDITORIA AL BALANCE	SI	SI	Informe de auditoría al balance general de la nación	Informe de auditoría al balance general de la nación, hallazgos presupuestales y contables y su calificación	Español	Medio magnético y/o físico	Archivos PDF/ medio impreso	Disponible en Archivo de Gestión de la Gerenteía Delegada para Economía y Finanzas Públicas para consulta en Gerenteía Delegada para Economía y Finanzas Públicas, y en http://www.Gerenteia.gov.co/web/guest/informesconstitucionales
PROGRAMACIÓN Y EJECUCIÓN PRESUPUESTAL	SI	SI	Categoria CGR_PRESUPUESTAL	Programaciones y ejecuciones presupuestales de ingreos y gastos del nivel territorial, empresas y sociedades con capital público	Español	Medio magnético	Hojas de cálculo	Publicada en la web http://www.chip.gov.co/schip_rt/ y disponible para consulta en Gerenteia Delegada para Economía y Finanzas Públicas
REGISTROS DE DEUDA NACIONAL	NO	SI	Deuda pública nacional	Registros de contratos de deuda pública y sus amortizaciones	Español	Medio magnético	Hojas de cálculo	Disponible en bases de datos para consulta en Gerenteía Delegada para Economía y Finanzas Públicas
REGISTROS DE DEUDA TERRITORIAL	NO	SI	Deuda pública territorial	Registros de contratos de deuda pública y sus amortizaciones	Español	Medio magnético	Hojas de cálculo	Disponible en basaes de datos para consulta en Gerenteía Delegada para Economía y Finanzas Públicas
INFORME ANUAL SOBRE LA DEUDA PÚBLICA	SI	SI	Situación de la deuda pública colombiana	Estado de la deuda pública nacional y territorial	Español	Medio magnético y/o físico	Archivos PDF / medio impreso	http://www.Gerenteia.gov.co/web/guest/informesconstitucionales y Dirección de Cuentas y Estadísticas Fiscales
CERTIFICACIONES DE REGISTRO DE LA DEUDA PÚBLICA NIVEL NACIONAL	NO	SI	Certificados de deuda pública	Certificacion de los registros de deuda pública nacional	Español	Medio Físico	Medio impreso	Disponible en Archivo de Gestión de la Gerenteía Delegada para Economía y Finanzas Públicas
CERTIFICACIONES DE REGISTRO DE LA DEUDA PÚBLICA NIVEL TERRITORIAL	NO	SI	Certificados de deuda pública	Certificacion de los registros de deuda pública territorial	Español	Medio magnético y/o físico	Hojas de cálculo	Disponible en Archivo de Gestión de la Gerenteía Delegada para Economía y Finanzas Públicas

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS								Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
CERTIFICACIONES PARA EL SALARIO DE LOS CONGRESISTAS	NO	SI	Incremento salarial de los congresistas	Cálculo del incremento salarial de los congresistas	Español	Medio magnético y/o físico	Documentos de texto / medio impreso	Disponible en Archivo de Gestión de la Gerenteía Delegada para Economía y Finanzas Públicas
INFORME ANUAL SOBRE LA CUENTA GENERAL DEL PRESUPUESTO Y DEL TESORO	SI	SI	Informe de cuenta general del presupuesto y del tesoro	Informe anual sobre la cuenta general del presupuesto y del tesoro	Español	Medio magnético y/o físico	Archivos PDF / medio impreso	Disponible en Archivo de Gestión de la Gerenteía Delegada para Economía y Finanzas Pública, para consulta en Gerenteía Delegada para Economía y Finanzas Públicas y en http://www.Gerenteia.gov.co/web/guest/informesconstitucionales
MARCO FISCAL DE MEDIANO PLAZO	No	SI	Marco Fiscal de Mediano Plazo	Proyeccion de 10 años de los ingresos y gastos del sector central territorial	Español	Medio magnético	Hojas de cálculo	Disponible para consulta en Gerenteía Delegada para Economía y Finanzas Públicas
PERSONAL Y COSTOS	No	SI	Personal y costos	Información anual sobre planta de personal de cada entidad	Español	Medio magnético	Hojas de cálculo	Disponible para consulta en Gerenteía Delegada para Economía y Finanzas Públicas
LIBRO DE LEGALIZACION DEL GASTO	No	SI	Libro de legalización del gasto	Información trimestral sobre los giros a legalizar y el recibo de bienes y servicios de dichos giros	Español	Medio magnético	Hojas de cálculo	Disponible para consulta en Gerenteía Delegada para Economía y Finanzas Públicas
INFORME ANUAL SOBRE LA SITUACIÓN DE LAS FINANZAS DEL ESTADO	SI	SI	Situación de las finanzas públicas	El estado de las finanzas consolidadas del Estado	Español	Medio magnético y/o físico	Archivos PDF / medio impreso	http://www.Gerenteia.gov.co/web/guest
INFORME FINANCIERO MENSUAL	SI	SI	Avance fiscal	Comportamiento fiscal mensual de las finanzas del Estado	Español	Medio magnético y/o físico	Archivos PDF / medio impreso	http://www.Gerenteia.gov.co/web/guest
BOLETIN FISCAL	SI	SI	Análisis Macro Fiscal	Análisis de coyuntura de diferentes sectores	Español	Medio magnético y/o físico	Archivos PDF / medio impreso	http://www.Gerenteia.gov.co/web/guest
ANALISIS DEL PRESUPUESTO GENERAL DE LA NACIÓN	SI	SI	Análisis del Presupuesto General de la Nación	Análisis Macroeconómico del Presupuesto General de la Nación	Español	Medio magnético y/o físico	Archivos PDF / medio impreso	http://www.Gerenteia.gov.co/web/guest
ESTUDIOS MACROECONOMICOS Y FISCALES	SI	SI	Estudios macrofiscales	Estudios sobre temas macroeconómicos y fiscales	Español	Medio magnético y/o físico	Archivos PDF / medio impreso	http://www.Gerenteia.gov.co/web/guest
ANALISIS DE PROYECTOS DE LEY	SI	SI	Análisis y evaluación de proyectos de ley que tengan impacto o incidencia macrofiscal	Estudios con los resultados de las evaluaciones de los proyectos de ley	Español	Medio magnético y/o físico	Archivos PDF / medio impreso	http://www.Gerenteia.gov.co/web/guest
RESOLUCIONES ORDINARIAS	No	SI	Resoluciones Ordinarias	Actos administrativos con los cuales se confiere comisión, se reconoce y ordena el pago de viáticos y transporte; se legalizan cajas menores, se autoriza el pago sentencias judiciales, entre otras.	Español	Físico	Doumento de texto	Archivo de Gestión de la Gerencia Administrativa y Financiera
SOLICITUDES DE VIÁTICOS	No	SI	Solicitudes de viáticos	Oficios mendiante los cuales las diferentes dependencias solicitan la autorización de los viáticos y transporte para los funcionarios que son comisionados en desarrollo de sus actividades para	Español	Físico	Doumento de texto	Archivo de Gestión de la Gerencia Administrativa y Financiera
PROYECTOS DE INVERSIÓN	SI	SI	Adquisición y Ampliación de la Infraestructura Física de laINSTITUTO NACIONAL DE MUSEOS	Proyecto de inversión formulado bajo el código BPIN 2012011000296, cuyo horizonte está entre el 2013 - 2018; para la adquisición y ampliación de la infraestructura física de la Gerenteía General de la República	Español	Análogo o digital - y Físicos	Documento de texto	Sistema para el Seguimiento a los Proyectos de Inversión - SPI, del Departamento Nacional de Planeación - DNP y físicos Archivo de Gestión de la Gerencia Administrativa y Financiera
CERTIFICADOS DE DISPONIBILIDAD PRESUPUESTAL			Certificados de disponibilidad presupuestal	Informacion relacionada con el presupuesto a ejecutar par determinado rubro contable	Español	Digital	PDF	SIIF NACIÓN
CERTIFICADOS DE RETENCIONES EN LA FUENTE			Certificados de retenciones en la fuente	Retenciones tributarias aplicadas a funcionaios, exfuncionarios y contratistas	Español	Digital	PDF	KACTUS, SIIF NACIÓN
DERECHOS DE PETICIÓN			Derechos de petición	Solicitudes de información de funcionarios y ciudadanos de acuerdoi al articulo 23 de la C.P.C	Español	Fisico	Texto	Archivo de Gestión de la Dirección Financiera y Archivo Central de la CGR

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS								Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
TUTELAS			Tutelas	Solicitudes de información de funcionarios y ciudadanos de acuerdoi a la C.P.C	Español	Fisico	Texto	Archivo de Gestión de la Dirección Financiera y Archivo Central de la CGR
INFORMES DE EJECUCIÓN PRESUPUESTAL			Informes de ejecución presupuestal	Documento en el que se decribe los gastos y la ejecucion de presupuesto	Español	Fisico	PDF	SIIF NACIÓN
INFORMES DE ESTADOS FINANCIEROS			Informes de estados financieros	Activos, pasivos y patrimonio, ingresos y gastos	Español	Fisico	PDF, Excel	Archivo de Gestión de la Dirección Financiera
INFORMES DE GESTIÓN			Informes de gestión	Informes de actividades realizadas por la Dirección	Español	Fisico	PDF, Excel, Papel	Archivo de Gestión de la Dirección Financiera
INFORMES DE OPERACIONES RECIPROCAS			Informes de operaciones reciprocas	Todas las operaciones que se tienen con Entidades del Estado	Español	Fisico	PDF, Excel, Word	Archivo de Gestión de la Dirección Financiera
INFORMES DE PASIVOS LABORALES			Informes de pasivos laborales	Acreencias con funcionarios y ex funcionarios	Español	Fisico	PDF, Excel, Word	Archivo de Gestión de la Dirección Financiera
INFORMES DE REPORTE DE INFORMACIÓN EXÓGENA			Informes de reporte de información exógena	Información referente a las retenciones que se efectúan a los proveedores	Español	Fisico	PDF, Excel, Word	Archivo de Gestión de la Dirección Financiera
LIBROS CONTABLES			Libros contables	Libros oficiales donde se registran los movimientos económicos de la Entidad	Español	Fisico	PDF, Excel, Word	Archivo de Gestión de la Dirección Financiera
COMPROBANTES DE CONTABILIDAD			Comprobantes de contabilidad	Documentos soportes de transacciones económicas con terceros	Español	Fisico	PDF, Excel, Word	Archivo de Gestión de la Dirección Financiera
LIBRO DIARIO			Libro diario	Libros oficiales donde se registran los movimientos económicos de la Entidad	Español	Fisico	PDF, Excel, Word	Archivo de Gestión de la Dirección Financiera
EXTRACTOS Y CONCILIACIONES BANCARIAS			Extractos y conciliaciones bancarias	Registro que envían los bancos de los movimientos de las cuentas de la CGR	Español	Fisico	PDF, Excel, Word	Archivo de Gestión de la Dirección Financiera
MOVIMIENTOS DE TESORERÍA			Movimientos de tesorería	Registro de las transacciones, pagos y descuentos que generan desembolsos de dinero	Español	Fisico	PDF, Excel, Word	Archivo de Gestión de la Dirección Financiera
BOLETINES DIARIOS			Boletines diarios	Registro de las transacciones, pagos y descuentos que generan desembolsos de dinero	Español	Fisico	PDF, Excel, Word	Archivo de Gestión de la Dirección Financiera
LEGALIZACIÓN DE VIÁTICOS			Legalización de viáticos	Certificaciones de cumplimiento y soportes de gastos de viaje en comisiones de trabajo de la CGR	Español	Fisico	Papel	Archivo de Gestión de la Dirección Financiera y Archivo Central de la CGR
LIBRANZAS			Libranzas	Documentos mediante los que los funcionarios autorizan descuentos por nomina	Español	Fisico	Papel	Archivo de Gestión de la Dirección Financiera y Archivo Central de la CGR
PAGO DE SENTENCIAS			Pago de sentencias	Registro contable de pagos por fallos judiciales de indemnizaciones pecuniarias a terceros	Español	Fisico	PDF, Excel, Word	Archivo de Gestión de la Dirección Financiera y Archivo Central de la CGR
TARIFA FISCAL			Tarifa fiscal	La tarifa que le adjudica la CGR por la cuota de auditaje	Español	Fisico	PDF, Excel, Word	Archivo de Gestión de la Dirección Financiera y Archivo Central de la CGR
TÍTULOS DE DEPÓSITOS JUDICIALES			Títulos de depósitos judiciales	Registro contable títulos valores que garantizan los cobros por responsabilidad fiscal a terceros	Español	Fisico	PDF, Excel, Word	Archivo de Gestión de la Dirección Financiera y Archivo Central de la CGR
ACTAS DE COMITE DE ARCHIVO	NO	SI	Actas de Comité de Archivo	Documentos que relacionan los temas tratados en las reuniones de Comité de Archivo de la Gerenteía General de la República	Español	Físico	Documento texto	Archivo de Gestión de la Dirección de Imprenta, Archivo y Correspondencia y Archivo Central de la Gerenteía General de la República
ACTAS DE ENTREGA DE DEPENDENCIA	NO	Se encuentran las actas y Formatos únicos de Inventario	Actas de entrega de dependencia	Son los documentos de entrega y recibo de los directivos de la Dirección de Imprenta, Archivo y Correspondencia sobre el Archivo de Gestión de la Dirección de Imprenta, Archivo y Correspondencia, Archivo de Gestión Centralizado y Archivo Central - Nivel Central	Español	Fisico	Papel	Archivo de Gestión de la Dirección de Imprenta, Archivo y Correspondencia

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS								Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
AUTENTICACIONES DOCUMENTALES	NO	NO	Autenticaciones documentales	Agrupación documental, que contiene los documentos (físicos y magnéticos) de las solicitudes de copias de documentos bajo custodia de la Dirección de Imprenta, Archivo y Correspondencia en los Archivos de Gestion Centralizado y Archivo Central - Nivel Central	Español	Fisico - Electronicos (Magneticos)	Papel generalmente carta. Electronicos (Magneticos): Reposan cuenta de correo o SIGEDOC	Archivo de Gestión Centralizado y Archivo Central - Nivel Central
CERTIFICACIONES DE PAZ Y SALVO DOCUMENTAL	NO	SI	Certificaciones de paz y salvo documental	Son las solicitudes y respuestas para el paz y salvo documental por parte de las dependencias del nivel central; los caules puesden ser en estado fisico o digital (Sistema de Gestión Documental). En los	Español	Fisico o electronico	Papel o digital	Archivo de Gestión de la Dirección de Imprenta, Archivo y Correspondencia
CONSECUTIVO DE COMUNICACIONES OFICIALES	NO	Se encuentran las copias de las comuniacciones oficiales	Consecutivo de comunicaciones oficiales	Son las comunicaciones oficiales enviadas en soporte papel, se elaborarán en original y máximo dos copias, remitiéndose el original al destinatario, la primera copia a la serie respectiva de la oficina que genera el documento, teniendo en cuenta los anexos correspondientes y la segunda copia reposará en el consecutivo de la unidad de correspondencia, por el tiempo establecido en su	Español	Fisico	Papel	Archivo de Gestión de la Dirección de Imprenta, Archivo y Correspondencia
CONSULTAS SOBRE GESTIÓN DOCUMENTAL Y ADMINISTRACIÓN DE ARCHIVOS	NO	Oficios, consultas telefónicas, visitas	Consultas sobre gestión documental y administración de archivos	Solicitudes y respuestas a consultas en materia de gestión documental del Nivel Central y Desconcentrado	Español	Fisico	Papel	Archivo de Gestión de la Dirección de Imprenta, Archivo y Correspondencia
PLANILLAS DE DEVOLUCION DE ENVIOS	NO	Planilla de	Planillas de devolución de envíos	Recopilación de las comunicaciones que no fueron entregadas por algún motivo (direccion errada, no vive, entre otros)	Español	Fisico	Papel	Archivo de Gestión de la Dirección de Imprenta, Archivo y Correspondencia
PLANILLA DE RECIBO DE ENVIOS	NO	Planillas	Planilla de recibo de envíos	Planilla de recibos envios entre Gerencias Departamentales Colegiadas y el Nivel Central	Español	Fisico	Papel	Archivo de Gestión de la Dirección de Imprenta, Archivo y Correspondencia
PLANILLAS DE ENVIOS	SIPOS	Planillas y \	Planillas de envíos	Planillas de envios de Nivel Central y Gerencias Departamentales Colegiadas, y Nivel Central a los usuarios externos	Español	Fisico y electrónico (Guías en SPN 4-72)	Papel	Archivo de Gestión de la Dirección de Imprenta, Archivo y Correspondencia y Página Web SPN 4-72
PRUEBAS DE ENTREGA	NO	Guía	Pruebas de entrega	Relación de las guias recibidas por usuarios externos	Español	Físico	Papel	Archivo de Gestión de la Dirección de Imprenta, Archivo y Correspondencia y Página Web SPN 4-72
INFORMES DE GESTIÓN DOCUMENTAL	NO	Informe	Informes de gestión documental	Relaciona las actividades semestrales de la Dirección de Imprenta, Archivo y Correspondencia	Español	Físico y electrónico	Papel	Archivo de Gestión de la Dirección de Imprenta, Archivo y Correspondencia
INFORMES DE GESTION DOCUMENTAL - ANUAL CONSOLIDADO GerenteIA GENERAL DE LA REPUBLICA	NO	Inventario	Informes de gestión documental - anual consolidado Gerenteía General de la República	Relaciona el inventario anual de los documentos del Nivel Central y Desconcentrado	Español	Físico y electrónico	Papel	Archivo de Gestión de la Dirección de Imprenta, Archivo y Correspondencia
INFORMES DE GESTIÓN DOCUMENTAL - SEMESTRAL CONSOLIDADO GerenteIA GENERAL DE LA REPUBLICA	NO	Informes	Informes de gestión documental Semestral consolidado Gerenteía	Relaciona los informes de gestión documental semestrales del Nivel Central y Desconcentrado anual	Español	Físico y electrónico	Papel	Archivo de Gestión de la Dirección de Imprenta, Archivo y Correspondencia
INFORMES DE SEGUIMIENTO CONVENIO ARCHIVO GENERAL DE LA NACION	NO	Unicamente se encuentra los oficios o formatos diligenciando la capacitación de los	Informes de seguimiento convenio Archivo General de la Nación	Se refiere a los documentos que tenga que ver con el convenio interadministrativo con el Archivo General de la Nación	Español	Físico	Papel	Archivo de Gestión de la Dirección de Imprenta, Archivo y Correspondencia año 2012 y 2013.

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS — **Versión 1.0**

CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
INVENTARIOS DE ENTREGAS DOCUMENTALES AL ARCHIVO GESTION CENTRALIZADO	NO	NO	Entregas Documentales	Es el Formato Único de Inventario Documental - FUID, firmado entre la dependencia del nivel central productora de los documentos y la Dirección de Impreta, Archivo y Correspondencia, en el que se registran los documentos que se entregan al Archivo de Gestión Centralizado y que entran a hacer parte de la misma unidad de información archivística. Se publica en la página Web de la Gerenteía General de la República, aplicando por analogia lo señalado en: Artículo 2.8.2.2.4., Decreto 1080 de 2015; Literal e), Artículo	Español	Físico - Electrónicos (Magnéticos)	Papel generalmente carta y oficio. Electrónicos (Magnéticos) contenidos en CD: Archivos en formato MS Excel.xls y PDF	Archivo de Gestion Centralizado (Nivel Central). La única parte disponible virtualmente es el Formato Unico de Inventario Documental - FUID, firmado entre la dependencia del Nivel Central productora de los documentos y la Dirección de Imprenta, Archivo y Correspondencia, en el link http://www.Gerenteiagen.gov.co/web/guest/gestion-documental
INVENTARIOS DE ELIMINACIONES DOCUMENTALES	SI	SI	Eliminación Documental	Es el Formato Único de Inventario Documental - FUID, debidamente firmado por parte de quienes intervinieron en su elaboración y el jefe de la dependencia del Nivel Central productora de los documentos y debidamente aprobado por el Comité de Archivo de la Gerenteía General de la República, en el que se registran los documentos a eliminar y eliminado. Se publica en la página Web, lo señalado, Articulo 2.8.2.2.5, Decreto 1080 de 2015; Artículo 15, Acuerdo AGN No. 004 de 2013 y Artículo 18 del Acuerdo AGN No. 003 de 2015.	Español	Físico - Electrónicos (Magnéticos)	Papel generalmente carta y oficio. Electrónicos (Magnéticos) contenidos en CD: Archivos en formato MS Excel.xls y PDF. Los publicados en la Web de laINSTITUTO NACIONAL DE MUSEOSen formato PDF	Archivo de Gestion Centralizado (Nivel Central). La única parte disponible virtualmente es el Formato Unico de Inventario Documental, FUID, que fue aprobado por parte de Comité de Archivo de la CGR, en el link http://www.Gerenteiagen.gov.co/web/guest/gestion-documental
INVENTARIOS DE TRANSFERENCIAS DOCUMENTALES PRIMARIAS	NO	NO	Transferencias Documentales Pri	Es el Formato Único de Inventario Documental - FUID, firmado entre la dependencia del Nivel Central productora de los documentos y la Dirección de Imprenta, Archivo y Correspondencia, en el que se registran los documentos Transfreridos al al Archivo Central y que entran a hacer parte de la misma unidad de información archivística. Se publica en la página Web, los señalado, Artículo 2.8.2.2.4., Decreto 1080 de 2015; Literal e), Artículo 2.8.2.5.8., Decreto 1080 de 2015; Articulo 11, Acuerdo Archivo General de la Nación No. 002 de 2014; Artículo 17 del Acuerdo AGN No. 005 de 2015.	Español	Físico - Electrónicos (Magnéticos)	Papel generalmente carta y oficio. Electrónicos (Magnéticos) contenidos en CD: Archivos en formato MS Excel.xls y PDF.	Archivo Central. La única parte disponible virtualmente es el Formato Único de Inventario Documental - FUID, firmado entre la dependencia del Nivel Central productora de los documentos y que transfiere y la Dirección de Imprenta, Archivo y Correspondencia, que se describe en la Categoría de Inventarios Documentales del presente Registro, en el link http://www.Gerenteiagen.gov.co/web/guest/gestion-documental
INVENTARIOS DOCUMENTALES	NO	NO	Inventarios Documentales	Es el Formato Único de Inventario Documental, FUID, firmado entre la dependencia del nivel central productora de los documentos y la DIAC, en el que se registran los documentos que se entregan al Archivo de Gestión Centralizado y los que han sido producto de Transferencias Primarias Documentales que entran a hacer parte del Archivo Central. Se publica en la pagina web, los señalado, Artículo 2.8.2.2.4., Decreto 1080 de 2015; Literal e), Artículo 2.8.2.5.8., Decreto 1080 de 2015; Articulo	Español	Fisico - Electronicos (Magneticos)	Papel generalmente carta y oficio. Electronicos (Magneticos) contenidos en CD: Archivos en formato MS excel.xls y PDF.	Archivo de Gestion Centralizado (Nivel Central). La única parte disponible virtualmente es el Formato Unico de Inventario Documental, FUID, firmado entre la dependencia del nivel central productora de los documentos y la DIAC, en el link http://www.Gerenteiagen.gov.co/web/guest/gestion-documental
INVENTARIOS DE ALMACÉN	N0	Reporte del aplicativo de recursos físicos	Inventarios de almacén	Se encuentran las novedades de traspasos y bajas de elementos devolutivos destinados para la Dirección de Imprenta, Archivo y Correspondencia	Español	Físico	Papel	Archivo de Gestión de la Dirección de Imprenta, Archivo y Correspondencia
PROGRAMA DE CAPACITACIÓN Y SENSIBILIZACIÓN EN GESTIÓN DOCUMENTAL	NO	Solo se encuentra planillas de	Programa de capacitación y sensibilización en gestión documental	Esta serie comtempla todas las capacitaciones efectuadas por la Dirección de Imprenta, Archivo y Correspondencia en materia de gestión documental tanto en el Nivel Central como Desconcentrado	Español	Físico	Papel	Archivo de Gestión de la Dirección de Imprenta, Archivo y Correspondencia

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS								Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
PROGRAMA DE ELIMINACIONES DOCUMENTALES	NO	NO	Eliminación Documental	Expediente agrupa los documentos generados durante el proceso de materializacion de las eliminaciones documentales por parte dependencias Nivel Central Gerenteía General de la República. Agrupa las instrucciones, acompañamiento y orientaciones impartidas a las Gerencias Departamentales Colegiadas de la Gerenteía General de la República. Se publica en la página Web, lo señalado en: Artículo 2.8.2.2.5, Decreto 1080 de 2015; Artículo 15, Acuerdo AGN No. 004 de 2013 y Artículo 18 del Acuerdo Archivo General de la Nación No. 003 de 2015	Español	Físico - Electrónicos (Magnéticos)	Papel generalmente carta y oficio. Electrónicos (Magnéticos) contenidos en CD: Archivos en formato MS Excel.xls y PDF. Los publicados en la Web de laINSTITUTO NACIONAL DE MUSEOSen formato PDF	Expediente Físico: - Archivo Central - De este expediente se publicara en la página web de la CGR en el link: http://www.Gerenteiagen.gov.co/web/guest/gestion-documental, lo correspondiente a los Ineventarios de Documentos a Eliminar y Eliminados.
PROGRAMA DE SEGUIMIENTO Y CONTROL DE LOS ARCHIVOS DE LA GerenteIA GENERAL DE LA REPUBLICA	NO	NO	Implementación Programa de Gestión Documental Gerenteía General de la República	Agrupación documental relacionada con la operativización de los procesos de gestión Documental (Planeación, Producción; Gestión y trámite; Organización; Transferencia; Disposición; Preservación a largo plazo y Valoración), que incluye las actividades de desarrollo de instrumentos y programas específicos de gestión documental y su armonización con el Sistema Integrado de Gestión y Control de Calidad -SIGCC y Programas gubernamentales (Gobierno en Línea, Cero Papel), Políticas públicas y buenas prácticas	Español	Físico - Electrónicos (Magnéticos)	Papel generalmente carta y oficio. Electrónicos (Magnéticos) contenidos en CD: Archivos en formato MS Excel.xls y PDF. Los publicados en la Web de laINSTITUTO NACIONAL DE MUSEOSen formato PDF	Expediente Físico: - Archivo Central - De este expediente se publicara en la página web de la CGR en el link, entre otros, los Instrumentos Archivisticos el Programa de Gestión Documental CGR, (TRD, Cuadros de Clasificacion Documental, Bancos Termnilogicos, PINAR y demas), Programas Especificos de Gestión Documental, los Registros de Activos de Información, acorde a los Artículos 2.8.5.1. 2,8.5.2; 2.8.5.1.1., 2.8.5.1.2.; Artículo 2.8.3.1.2. Decreto 1080 de 2015. : http://www.Gerenteiagen.gov.co/web/guest/gestion-documental.
PROGRAMA DE TRANSFERENCIAS DOCUMENTALES	NO	NO	Entregas Documentales	Expediente que agrupa los documentos generados durante el proceso de entrega y transferencias primarias documentales por parte dependencias Nivel Central Gerenteía Genenral de la República al Archivo de Gestión Centralizado y al Archivo Central respectivamente. Incluye documentos de planificación, aprobación, socialización y acompañamiento a cada una de las dependencias por parte de los asesores documentales designados por la Dirección de Imprenta, Archivo y	Español	Físico - Electrónicos (Magnéticos)	Papel generalmente carta y oficio. Electrónicos (Magnéticos) contenidos en CD: Archivos en formato MS Excel.xls y PDF	Archivo de Gestion Centralizado (Nivel Central). La única parte disponible virtualmente es el Formato Unico de Inventario Documental, FUID, firmado entre la dependencia del nivel central productora de los documentos y la DIAC, que se describe en la Categoría de *Inventarios Documentales* del presente Registro.
REGISTRO DE CONTROL DE CONSULTA	NO	SI	Registro de control de consulta	Documentos que relacionan las consultas de documentos que se encuentran en el Archivo de Gestión de la Dirección de Imprenta, Archivo y	Español	Físico	Documento texto	Archivo de Gestión de la Dirección de Imprenta, Archivo y Correspondencia
REGISTRO DE CONTROL DE PRÉSTAMO	NO	SI	Registro de control de préstamo	Documentos que relacionan los prestamos de documentos que se encuentran en el Archivo de Gestión de la Dirección de Imprenta, Archivo y	Español	Físico	Documento texto	Archivo de Gestión de la Dirección de Imprenta, Archivo y Correspondencia
REGISTRO DE CONTROL DE REPROGRAFÍA	NO	SI	Registro de control de reprografía	Documentos que relacionan el servicio de reprografía de documentos que se encuentran en el Archivo de Gestión de la Dirección de Imprenta,	Español	Físico	Documento texto	Archivo de Gestión de la Dirección de Imprenta, Archivo y Correspondencia
SEGUIMIENTO AL SISTEMA DE INFORMACIÓN DE GESTIÓN DOCUMENTAL	NO	Oficios de seguimiento Sigedoc	Seguimiento al sistema de información de gestión documental	Toda la información solicitada por los usuarios tanto del Nivel Central como Desconcentrado y las respuestas dadas por la Dirección de Imprenta,	Español	Físico	Papel	Archivo de Gestión de la Dirección de Imprenta, Archivo y Correspondencia
SUMINISTRO DE INSUMOS DE ELEMENTOS	N0	Reporte de insumos	Inventarios de almacén	Se encuentran las novedades de entrega de elementos para el manejo de los documentos de archivos del Nivel Central y Desconcentrado	Español	Fisico	Papel	Archivo de Gestión de la Dirección de Imprenta, Archivo y Correspondencia
TABLAS DE RETENCION DOCUMENTAL	NO	SI	Tablas de retención documental	Documentos que relacionan las series, subseries y tipos documentales producidos y recibidos por cada dependencia de la Gerenteía General de la República, en cumplimiento de sus funciones	Español	Físico	Documento texto	Archivo de Gestión de la Dirección de Imprenta, Archivo y Correspondencia y Archivo Central de la CGR. http://www.Gerenteiagen.gov.co/web/guest/gestion-documental

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS **Versión 1.0**

CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
JUNTA DE ADQUISICIONES DEL NIVEL CENTRAL	NO	SI	Junta de adquisiciones del Nivel Central	Actas de la junta de adquisiciones, por medio de la cual se recomienda el inicio o no de un proceso de contratación según el caso	Español	Físico	Papel	Dirección de Recursos Físicos
CERTIFICACIONES DE CONTRATOS	NO	SI	Certificaciones de contratos	Documento de constancia, sobre la suscripción de un contrato con los datos más relevantes, ya sea en ejecución o ejecutados, tanto de persona natural	Español	Físico	Papel	Dirección de Recursos Físicos
COMPROBANTE DE BAJA DE BIENES NIVEL CENTRAL	NO	SI	Comprobante de baja de bienes Nivel Central	Documento mediante el cual se retira un bien devolutivo del inventario de la Gerenteía General de la República	Español	Físico	Papel	Dirección de Recursos Físicos
CONTRATOS	SI	SI	Contratos	Relación de los contratos celebrados por la Gerenteía General de la República, ya sea de la actual vigencia o anteriores	Español	Físico y Digital	Papel - PDF	Dirección de Recursos Físicos
DEREHOS DE PETICION	NO	SI	Derechos de petición	Derechos de petición tramitados por la Dirección de Recursos Físicos	Español	Físico	Papel	Dirección de Recursos Físicos
TUTELAS	NO	SI	Tutelas	Tutelas tramitadas por la Dirección de Recursos Físicos	Español	Físico	Papel	Dirección de Recursos Físicos
HOJA DE VIDA DE INMUEBLES	NO	SI	Hoja de vida de inmuebles	Etapas pre y contractuales incluidas las escrituras referentes a la propiedad y uso de los diferentes inmuebles de la Entidad	Español	Físico	Papel	Dirección de Recursos Físicos
HOJA DE VIDA DE VEHÍCULOS	NO	SI	Hoja de vida de vehículos	Etapas pre y contractuales incluidas propiedad, seguros y mantenimientos de los diferentes vehículos al servicios de la Entidad	Español	Físico	Papel	Dirección de Recursos Físicos
INFORMES DE GESTIÓN	NO	SI	Informes de gestión	Información referente a los diferentes procesos adelantados por la Dirección según la normatividad vigente	Español	Físico	Papel	Dirección de Recursos Físicos
INVENTARIO DE ELEMENTOS DEVOLUTIVOS POR DEPENDENCIAS	NO	SI	Inventario de elementos devolutivos por dependencias	Relación con los datos principales de los elementos devolutivos asignados a las diferentes dependencias de la Entidad	Español	Físico	Papel	Dirección de Recursos Físicos
PLAN DE COMPRAS	SI	SI	Plan de compras	Plan anual de adquisiciones en donde se incorporan las diferentes compras de bienes y/o servicios para las labores inherentes de la Entidad	Español	Físico y Digital	Papel - PDF	Dirección de Recursos Físicos
PROCESOS DE CONTRATACIÓN DECLARADOS DESIERTOS	NO	SI	Procesos de contratación declarados desiertos	Procesos de contratación adelantados por la entidad los cuales por alguna circunstancia no pudieron ser adjudicados	Español	Físico	Papel	Dirección de Recursos Físicos
SUPERVISIÓN DE CONTRATOS	SI	SI	Supervisión de contratos	Documento mediante el cual los supervisores informan sobre el avance, calidad, cumplimiento entre otras, de los contratos suscritos por la	Español	Físico y Digital	Papel - PDF	Dirección de Recursos Físicos
HISTORIAS LABORALES	Perfil de funci	Petil Funcionarios principales	Perfil funcionarios principales	Nombres Cargo Perfil	Español	Electrónico	Electrónico	Datos funcionarios principales
NÓMINA	Decreto Salarial	Decreto Sal	Nómina	Decreto Salarial vigente expedido por el Gobierno Nacional, por la cual se fijan las escalas de remuneración correspondientes a las distintas categorías de los empleos de la Gerenteía General	Español	Digital	PDF	Decreto Salarial anual
RESOLUCIONES ORDINARIAS	Resoluciones de Nombramientos	Resoluciones de Nombramientos de la vigencia	Resoluciones de Nombramiento	Resoluciones ordinarias de nombramiento de los funcionarios que ingresan a la entidad durante la vigencia.	Español	Digital	PDF	Resoluciones de nombramiento funcionarios CGR
PROCESO DE CONCURSO DE SELECCIÓN DE PERSONAL	Concurso de méritos	Información del Proceso de Selección de	Concurso de Méritos de la vigencia	Convocatoria, información relacionada con el proceso y resultados de cada etapa del concurso de méritos para proveer cargos de carrera administrativa.	Español	Electrónico	PDF	Convocatoria, información del concurso de méritos para selección de personal de carrera
MANUAL DE FUNCIONES POR COMPETENCIAS LABORALES	Manual de Funci	Manual Específico de Funciones	Manual de Funciones por Competencias Laborales	El Manual de Funciones por Compencias Laborales contiene la identificación, propósito, funciones escenciales, contribuciones y requisitos de estudio y experiencia de los cargos de la Gerenteía General.	Español	Electrónico	PDF	Manual Específico de Funciones por Competencias Laborales Vigente
ACCIONES O REQUERIMIENTOS JUDICIALES	SI (Página Web) es necesario revisar la	SI con excepciones	Acciones o requerimientos judiciales	Demandas, solicitudes y/o requerimientos emanados de autoridad judicial; y su correspondiente respuesta	Español	Medio magnetico	PDF	Esta disponible en medio magnetico la que este relacionada con la acción o requerimiento judicial, en la Oficina Juridica como dependencia coordinadora de la respuesta.

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS								Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB.	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
ACTAS DE AYUDAS DE MEMORIA	NO	SI con excepciones	Actas o papeles de trabajo	Las actas recojen los compromisos y actividades de trabajo	Español	Papel - Medio magnetico: Procesador de palabra y documentos powerpoint, PDF, entre otros medios ofimaticos.	Fisicos o Analogos: Son documentos en formato tamaño carta y oficio (ANEXOS). Magneticos o Electronicos: Estan en procesador de palabra word.doc, Power point, excel.xls, PDF entre otros.	Esta disponible en medios magneticos en el Despacho del Gerente Delegado para la Participación Ciuadadana
ACTAS DE COMITÉ TÉCNICO	NO	SI	Actas	Las acta recojen las decisiones del Comité Técnico de la CD Para la Participación Ciudadana, en lo que hace Plan de Accion, Plan Anticorrupción; Plan de Mejoramiento, seguimiento a las metas y gestión del despacho y las dos direcciones.	Español	Papel - Medio magnetico: Procesador de palabra y documentos powerpoint, PDF, entre otros medios ofimáticos.	Fisicos o Analogos: Son documentos en formato tamaño carta y oficio (ANEXOS). Magneticos o Electronicos: Estan en procesador de palabra word.doc, Power point, excel.xls, PDF entre otros.	Esta disponible en medios magneticos en el Despacho del Gerente Delegado para la Participación Ciuadadana
INFORMES DE ESPECIAL SEGUIMIENTO	Sí	Sí	Informes	Resultados del trabajo de especial seguimiento sobre los recursos al Fondo Adaptación y la Unidad de Gestión del Riesgo	Español	Papel - Medio magnético	Fisicos o Analogos: Son documentos en formato tamaño carta y oficio (ANEXOS). Magneticos o Electronicos: Estan en procesador de palabra word.doc, Power point, excel.xls, PDF entre otros.	Esta disponible en medios magneticos en el Despacho del Gerente Delegado para la Participación Ciuadadana y los informes publicados en la página web de la entidad
DENUNCIAS	SI	SI - Link Denuncias en la página	Sistema de Información de Participación Ciudadana - SIPAR	Formularios de acceso al ciudadano para el registro, actualización y consulta de sus derechos de petición	Español	Electrónico	Página Web	Derechos de petición presentados de forma exclusiva a cada usuario (ciudadano) registrado
DERECHOS DE PETICIÓN	SI	SI	Trámites y servicios al ciudadano	Publicación de los diferentes trámites que la CGR presta al ciudadano y los protocolos de acceso, junto con el proceso general de atención de los derechos de petición	Español	Electrónico	Página Web	Contenido publicado en la página

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS								Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
TUTELAS	NO	SI (Dirección de Atención Ciudadana)	Tutela	Respuesta al escrito de tutela en los temas competentes en la Dirección de Atención Ciudadana	Español	Papel-Medio magnetico	Fisicos o Analogos: Son documentos en formato tamaño carta y oficio (ANEXOS). Magneticos o Electronicos: Estan en procesador de palabra word.doc y PDF	Esta disponible en medios magneticos y físico en la Dirección de Atención Ciudadana
INFORMES DE GESTIÓN	No	Sí	Informes	Descripción detallada del cumplimiento de las metas del Plan de Acción y de los resultados obtenidos por la gestión del despacho y las dos direcciones dentro del proceso Desarrollar el Control Fiscal Participativo	Español	Papel - Medio magnético	Fisicos o Analogos: Son documentos en formato tamaño carta y oficio (ANEXOS). Magneticos o Electronicos: Estan en procesador de palabra word.doc, Power point, excel.xls, PDF entre otros.	Esta disponible en medios magneticos en el Despacho del Gerente Delegado para la Participación Ciuadadana
INFORMES DEL CENTRO DE ATENCIÓN INTEGRAL AL CIUDADANO - CAIC	Sí	Sí	Informes	Descripción de la atención realizada en el Centro de Atención al Ciudadano del nivel central	Español	Papel - Medio magnético	Fisicos o Analogos: Son documentos en formato tamaño carta y oficio (ANEXOS). Magneticos o Electronicos	Esta disponible en medios magneticos en el Despacho y los informes publicados en la página web de la entidad.
INFORMES EVENTUALES	NO	SI	Informes	De acuerdo con el tema analizado o desarrollado	Español	Papel - Medio magnético	Fisicos o Analogos: Son documentos en formato tamaño carta y oficio (ANEXOS). Magneticos o Electronicos	Esta disponible en medio físico y magnetico en el Despacho
INFORMES GENERADOS POR ACTIVIDADES ESPECIALES ASIGNADAS AL DESPACHO	NO	SI	Informes	De acuerdo con el tema analizado o desarrollado	Español	Papel - Medio magnético	Fisicos o Analogos: Son documentos en formato tamaño carta y oficio (ANEXOS). Magneticos o Electronicos	Esta disponible en medio físico y magnetico en el Despacho
INFORMES PARA EL PLAN DE GESTIÓN DE LA INFORMACIÓN ESTRATEGICA	SI (Pagina web)	SI	Informes	Acciones y estrategias	Español	Papel-Medio magnetico	Fisicos o Analogos: Son documentos en formato tamaño carta y oficio (ANEXOS). Magneticos o Electronicos	Esta disponible en medio físico y magnetico en el Despacho

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS								Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
INFORMES SEMESTRALES CONSOLIDADOS DE MEDICION DE LA SATISFACCION DEL CLIENTE NIVEL NACIONAL	SI (Página Web)	SI	Informes	Resultados cualitativos y cuantitativos de la medición de la satisfacción del cliente sobre la información recogida en los instrumentos aplicados en las orientaciones realizadas a los ciudadanos en el CAIC.	Español	Papel - Medio magnetico: Procesador de palabra y documentos PDF.	Físicos y análogos	Sí
ACTAS DE OBSERVATORIO TRIMESTRAL DE DERECHOS DE PETICIÓN	NO	SI	Informe de observatorio trimestral consolidado por la Dirección de Atención Ciudadana	Análisis del estado de los derechos de petición de vigencias anteriores a la fecha de desarrollo del observatorio	Español	Físico y electrónico	PDF y Físico	SI
INFORMES CONSOLIDADOS DE AUDITORIAS ARTICULADAS	SI	SI	Informe semestral y/o anual de gestión a nivel nacional por la Gerenteía General de la República- Auditorías articuladas	Informe cuantitativo y cualitativo del desarrollo de la estrategia de auditorías articuladas	Español	Físico y electrónico	PDF y Físico	Publicada en la página Web de la CGR
INFORMES DE SUPERVISION MENSUAL	NO	SI	Informe de supervisión mensual consolidado por la Dirección de Atención Ciudadana	Análisis de la atención de los derechos de petición a nivel nacional para cada periódo mensual	Español	Físico y electrónico	PDF y Físico	SI
INFORMES CONSOLIDADOS DE EVALUACIÓN DE LA SATISFACCIÓN DEL CLIENTE CIUDADANÍA CUNDINAMARCA Y BOGOTÁ	SI (Página Web)	SI	Informes	Resultados cualitativos y cuantitativos de la medición de la satisfacción del cliente sobre la información recogida en los instrumentos aplicados en las actividades de promoción y desarrollo del nivel central.	Español	Papel - Medio magnetico: Procesador de palabra y documentos PDF.	Físicos y análogos	Sí
INFORMES CONSOLIDADOS DE SUPERVISIÓN Y SEGUIMIENTO NACIONAL	No	Si	Informes	Supervisión al cumplimiento de los tiempos establecidos en el Procedimiento Actividades de Promoción y Desarrollo del Control Ciudadano y seguimiento a la ejecución de los programas de	Español	Papel - HTML Aplicativo SIPAR	Físicos y análogos	Sí
INFORMES CONSOLIDADOS SATISFACCIÓN DEL CLIENTE CIUDADANIA	SI (Página Web)	SI	Informes	Resultados cualitativos y cuantitativos de la medición de la satisfacción del cliente sobre la información recogida en los instrumentos aplicados en las actividades de promoción y desarrollo del nivel central y desconcentrado.	Español	Papel - Medio magnetico: Procesador de palabra y documentos PDF.	Físicos y análogos	Sí
INVESTIGACIONES EN PARTICIPACIÓN CIUDADANA	Sí	Sí	Publicaciones	Resultados de las investigaciones realizadas por la Dirección de Promoción y Desarrollo en cumplimiento del artículo 57 del Decreto Ley 267	Español	Papel	Físicos - Libros y cartillas	Sí
PROCESO PARA ELABORACION DE DOCUMENTOS ESCRITOS DE PARTICIPACIÓN CIUDADANA	No	Sí	Documentos escritos - Producción de información dentro de la esfera de lo público	Documentos requeridos para la gestión de la dependencia que surten los pasos establecidos en el Procedimiento "Elaboración de documentos escritos de participación ciudadana"	Español	Papel - Medio magnético	Físicos y análogos	Sí
PROGRAMAS DE PROMOCIÓN Y DESARROLLO DEL CONTROL CIUDADANO	No	Sí	Producción de información dentro de la esfera de lo público	Documentos requeridos para la gestión de la dependencia que surten los pasos establecidos en el Procedimiento "Elaboración de documentos escritos de participación ciudadana"	Español	Papel - Medio magnético	Físicos y análogos	Sí
REGISTROS DE LAS ACTIVIDADES DE PROMOCIÓN Y DESARROLLO DEL CONTROL CIUDADANO	No	Sí con excepciones	Registros	Registros físicos y virtuales (aplicativo SIPAR) estipulados en el procedimiento "Actividades de Promoción y Desarrollo del Control Ciudadano"	Español	Papel - HTML Aplicativo SIPAR	Físicos y análogos	Sí con excepciones (datos sensibles en los listados de asistencia)
VEEDURIAS CIUDADANAS Y OTRAS FORMAS DE CONTROL SOCIAL A LA GESTIÓN PUBLICA	No	Sí con excepciones	Registros	Registros físicos y virtuales (aplicativo SIPAR) estipulados en el procedimiento "Actividades de Promoción y Desarrollo del Control Ciudadano"	Español	Papel - HTML Aplicativo SIPAR	Físicos y análogos	Sí con excepciones (datos sensibles en los listados de asistencia)
REPORTES DE ACCIÓN CIVIL DE ENTIDADES ORDEN NACIONAL	No	No	Reportes de acción civil de entidades orden nacional	Informes de gestión de apoderados de parte civil o incidente de reparación integral de la	Español	Físico o electrónico	Documento de texto o medio electrónico	No
REPORTES DE ACCIÓN CIVIL Gerenteía GENERAL DE LA REPÚBLICA	No	No	Reportes de acción civil Gerenteía General de la República	Informes de gestión de apoderados de parte civil o incidente de reparación integral de las Gerencias Departamentales Colegiadas. Ley 610 de 2000, Artículo 65	Español	Físico o electrónico	Documento de texto o medio electrónico	No
APERTURA DE PROCESOS PENALES	No	No	Apertura de procesos penales	Despacho judiciales reportan el avocamiento de preliminar o de instrucción en procesos que involucran dineros en delitos contra la Administración Pública. Código de Procedimiento	Español	Físico	Documento texto	No
SOLICITUD SOPORTES PARA LEGALIZACIÓN DE PODERES	No	No	Solicitud de soportes para legalización de poderes	Medio físico o electrónico que da base al otorgamiento del poder	Español	Físico o electrónico	Documento de texto o medio electrónico	No
ACTAS DE COMITÉ INTERNO	No	Si	Actas de Comité Interno	De seguimiento de actuaciones procesales, para unificar criterios jurídicos sobre responsabilidad fiscal, acciones de PMI y PA	Español	Físico	Documento de texto	Archivo de Gestión del Despacho del Gerente Delegado de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS								Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
ANTECEDENTES FISCALES	No	Si	Antecedentes fiscales	Hallazgos provenientes de auditoría, actuaciones especiales y/o denuncias	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de Gestión del Despacho del Gerente Delegado de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva
BOLETÍN DE RESONSABLES FISCALES	Si	Si	Boletín de Responsables Fiscales	Registro de responsables fiscales del orden nacional y territorial	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de Gestión del Despacho del Gerente Delegado de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva
EXCLUSIÓN DEL BOLETÍN DE RESPONSABLES FISCALES	Si	Si	Exclusión del Boletín de Responsables Fiscales	Retiro del Boletín cuando se acredita causal de exclusión	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de Gestión del Despacho del Gerente Delegado de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva
INCLUSIÓN AL BOLETÍNDE RESPONSABLES FISCALES	Si	Si	Inclusión al Boletín de Responsables Fiscales	Inclusión de personas naturales o jurídicas que tienen fallo con responsabilidad fiscal ejecutoriado y no pagado	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de Gestión del Despacho del Gerente Delegado de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva
SOLICITUDES RRELACIONADAS CON EL BOLETÍN DE RESPONSABLES FISCALES	No	Si	Solicitude relacionadas con el Boletín de Responsables Fiscales	Información sobre existencia de registros en antecedentes de responsabilidad fiscal, actualización de base de datos por cambio de nombre, aclaraciones sobre inhabilidades por registro en el Boletín de Responsables Fiscales.	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de Gestión del Despacho del Gerente Delegado de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva
CONSULTAS SOBRE ANTECEDENTES	No	Si	Consultas sobre antecedentes	Consulta	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de Gestión del Despacho del Gerente Delegado de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva
CONSULTAS SOBRE INDAGACIONES PRELIMINARES	No	Si	Consultas sobre indagaciones preliminares	Consulta	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de Gestión del Despacho del Gerente Delegado de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva
CONSULTAS SOBRE PROCESOS ADMINISTRATIVOS DE COBRO COACTIVO	No	Si	Consultas sobre procesos administrativos de cobro coactivos	Consulta	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de Gestión del Despacho del Gerente Delegado de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva
CONSULTAS SOBRE PROCESOS DE RESPONSABILIDAD FISCAL	No	Si	Consultas sobre procesos de responsabilidad fiscal	Consulta	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de Gestión del Despacho del Gerente Delegado de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva
COMUNICACIONES INFORMATIVAS	No	Si	Comunicaciones informativas	Internas y externas	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de Gestión del Despacho del Gerente Delegado de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva
CONTROL DE ASISTENCIA	No	Si	Control de asistencia	Planillas	Español	Físico	Documento texto	Archivo de Gestión del Despacho del Gerente Delegado de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva
CONTROL DE COMUNICACIONES OFICIALES	No	Si	Control de comunicaciones oficiales	En cuanto a su envío o su recepción	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de Gestión del Despacho del Gerente Delegado de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva
CONTROL DE ENTREGA DE COMUNICACIONES OFICALES	No	Si	Control de entrega de comunicaciones oficiales	Constancia registro electrónico en SIGEDOC y en físico	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de Gestión del Despacho del Gerente Delegado de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS								Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
DEVOLUCIONES DILIGENCIAS TRAMITADAS	No	Si	Devoluciones diligencias tramitadas	Las auxiliadas por Secretaría Común Conjunta	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de Gestión del Despacho del Gerente Delegado de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva
DERECHOS DE PETICIÓN	No	Si	Derechos de petición	Derechos de petición o solicitudes de información o documentos diferentes a los ingresados por SIPAR	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de Gestión del Despacho del Gerente Delegado de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva
TUTELAS	No	Si	Tutelas	Acción judicial para proteger derechos fundamentales	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de Gestión del Despacho del Gerente Delegado de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva
INDAGACIONES PRELIMINARES	No	Si	Indagaciones preliminares	Actuaciones para establecer daño fiscal y su cuantificación y/o presuntos responsables y/o nexo de causalidad	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de Gestión del Despacho del Gerente Delegado de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva
INFORMES DE APOYO TÉCNICO	No	No	Informes de apoyo técnico	Apoyo técnico dentro de actuaciones preliminares o de responsabilidad fiscal	Español	Físico y electrónico	Documento de texto y medio electrónico	Informe contenido dentro de la actuación preliminar o procesal
INFORMES DE COMISIONES DE SERVICIO	No	Si	Informes de comisiones de servicio	Informes de cumplido de las comisiones de los funcionarios de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de Gestión del Despacho del Gerente Delegado de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva
INFORMES DE DELEGACIONES	No	Si	Informes de delegaciones	Informes pormenorizados de los contratos y su ejecución, en los que el Delegado es asignado como supervisior	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de Gestión del Despacho del Gerente Delegado de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva
INFORMES DE GESTIÓN	No	Si	Informes de gestión	Información detallada sobre actividad desarrollada por el macroproceso de responsabilidad fiscal y su avance	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de Gestión del Despacho del Gerente Delegado de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva
LIBROS RADICADORES	No	Si	Libros radicadores	De asignaciones, autos, trámites de Secretaría Común	Español	Físico	Documento de texto	Archivo de Gestión del Despacho del Gerente Delegado de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva
NOTIFICACIONES POR ESTADO	No	Si	Notificaciones por estado	Publicación del respectivo acto administrativo según la Ley 1474 de 2011, Artículo 106	Español	Físico y electrónico	Documento de texto y medio electrónico	Secretaría Común Conjunta adscrita al Despacho de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva
OFICIOS DE CITACIONES	No	Si	Oficios de citaciones	Se emiten por los Abogados Sustanciadores o por la Secretaría Común Conjunta. En este último caso, por desconocimiento del domicilio del por notificar	Español	Físico y electrónico	Documento de texto y medio electrónico	Secretaría Común Conjunta adscrita al Despacho de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva o el Despacho mismo
PROCESOS DE RESPONSABILIDAD FISCAL	No	Si	Procesos de responsabilidad fiscal	Investigación dirigida a probar la existencia o no de daño fiscal y su cuantificación, producido por dolo o culpa de quien ejerce gestión fiscal o con ocasión de ésta, cuya decisión se contiene en un fallo	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de Gestión del Despacho del Gerente Delegado de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva
PROYECTOS DE RESOLUCIONES DE COMISIONES	No	Si	Proyectos de resoluciones de comisiones	Resoluciones de comisión a los funcionarios del Despacho de la Delegada para Investigaciones y de los Grupos de Investigaciones de las Gerencias Departamentales Colegiadas	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de Gestión del Despacho del Gerente Delegado de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva
REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS								Versión 1.0

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS								Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
PROYECTOS DE RESOLUCIONES DE SUSPENSIÓN DE FUNCIONARIOS PÚBLICOS	No	Si	Proyectos de resoluciones de suspensión de funcionarios públicos	Casos en que aplica el principio de verdad sabida y buena fe guardada del Art. 268-8 de la C.P.	Español	Físico	Documento de texto	Archivo de Gestión del Despacho del Gerente Delegado de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva
RESOLUCIONES DE EXCLUSIÓN, MODIFICACIONES O ACLARACIÓN DEL BOLETÍN DE RESPONSABILIDAD FISCAL	No	Si	Resoluciones de exclusión, modificaciones o aclaración del Boletín de Responsabilidad Fiscal	Exclusiones, modificaciones o aclaraciones de los registros del Boletín de Responsables Fiscales	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de Gestión del Despacho del Gerente Delegado de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva
REMISIÓN NOTIFICACIONES POR AVISO	No	Si	Remisión notificaciones por aviso	Se surte cuando no es posible la notificación personal.	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de Gestión del Despacho del Gerente Delegado de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva
SOLICITUDES DE APOYO	No	Si	Solicitudes de apoyo	Hacia o desde Gerencias Departamentales para notificaciones, toma de exposiciones libres o declaraciones juramentadas. En otro sentido, para obtener conceptos técnicos	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de Gestión del Despacho del Gerente Delegado de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva
SUPERVISIÓN DE CONTRATOS	No	Si	Supervisión de contratos	Contratos en que el Gerente Delegado para Investigaciones es el supervisor	Español	Físico	Documento de texto	Archivo de Gestión del Despacho del Gerente Delegado de la Gerenteía Delegada para Investigaciones, Juicios Fiscales y Jurisdicción Coactiva
ANTECEDENTES FISCALES	No	Si	Antecedentes fiscales	Hallazgos provenientes de auditoría, actuaciones especiales y/o denuncias	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de la Dirección de Investigaciones Fiscales
COMUNICACIONES INFORMATIVAS	No	Si	Comunicaciones informativas	Internas o externas	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de la Dirección de Investigaciones Fiscales
CONTROL DE ASISTENCIA	No	Si	Comunicaciones informativas	Internas o externas	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de la Dirección de Investigaciones Fiscales
CONTROL DE ENTREGA DE COMUNICACIONES OFICIALES	No	Si	Comunicaciones informativas	Internas o externas	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de la Dirección de Investigaciones Fiscales
DERECHOS DE PETICIÓN	No	Si	Derechos de petición	Derechos de petición o solicitudes de información o documentos diferentes a los ingresados por SIPAR	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de la Dirección de Investigaciones Fiscales
TUTELAS	No	Si	Tutelas	Acción judicial para proteger derechos fundamentales	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de la Dirección de Investigaciones Fiscales
INDAGACIONES PRELIMINARES	No	Si (Excepcionalmente, cuando	Indagaciones preliminares	Actuacion Preprocesal, iniciada de oficio para establecer la existencia de daño, presuntos autoires del mismo, competencia del organo fiscalizador	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de la Dirección de Investigaciones Fiscales
INFORMES DE GESTIÓN	No	Si	Informes de gestión	Información detallada sobre actividad desarrollada por el macroproceso de resposabilidad fiscal y su avance	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de la Dirección de Investigaciones Fiscales
LIBROS RADICADORES	No	Si	Libros radicadores	De asignaciones, autos, trámites de Secretaría Común	Español	Físico	Documento de texto	Archivo de la Dirección de Investigaciones Fiscales
PROCESOS DE RESPONSABILIDAD FISCAL	No	Si (Opera la reserva de la Art. de la Ley 610/2000, la que, según sentencia C-477 de 2001, se levanta	Procesos de responsabilidad fiscal	Investigación dirigida a establecer la responsabilidad fiscal de las personas que en ejercicio de la Gestion fiscal causaron daño al erario publico por una conducta Dolosa o gravemente culposa	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de la Dirección de Investigaciones Fiscales

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS									Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
TÍTULOS DE DEPÓSITOS JUDICIALES INVESTIGACIONES	No	Si	Titulos Judiciales	Son en resultado de las medidas cautelares decretadas dentro de los proceso de responsabilidad fiscal	Español	Físico y electronico		Archivo de la Dirección de Investigaciones Fiscales
ACTAS DE ENTREGA DE DEPENDENCIA	No	Si	Actas entrega de Dependencia	Corresponde a los documentos e informe de gestión que se entrega cuando hay cambio de directivo	Español	Físico y electrónico	Documento de texto y electrónico	Archivo Dirección de Juicios Fiscales
COMUNICACIONES INFORMATIVAS	No	Si	Comunicaciones informativas	Internas o externas	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo Dirección de Juicios Fiscales
CONTROL DE ASISTENCIA	No	Si	Control de asistencia	Planillas	Español	Físico	Documento de texto	Archivo Dirección de Juicios Fiscales
CONTROL DE COMUNICACIONES OFICIALES	No	Si	Control de comunicaciones oficiales	En cuanto a su envío o su recepción	Español	Físico y electrónico SIGEDOC	Documento de texto y medio electrónico	Archivo Dirección de Juicios Fiscales y SIGEDOC
CONTROL DE ENTREGA DE COMUNICACIONES OFICIALES	No	Si	Control de entrega de comunicaciones oficiales	Constancia registro electrónico (SIGEDOC) y en físico	Español	Físico y electrónico (SIGEDOC)	Documento de texto y medio electrónico	Archivo Dirección de Juicios Fiscales y SIGEDOC
DERECHOS DE PETICIÓN	No	Si	Derechos de petición	Derechos de petición o solicitudes de información ingresados por SIPAR o allegados directamente a la Dirección	Español	Físico y electrónico (SIPAR)	Documento de texto y medio electrónico	Archivo Dirección de Juicios Fiscales o SIPAR
TUTELAS	No	Si	Tutelas	Acción judicial para proteger derechos fundamentales	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo Dirección de Juicios Fiscales o SIPAR
INFORMES CUBO (SIREF)	No	No	Información SIREF	Información relacionada con la segunda instancia	Español	Físico y electrónico (SIREF)	Documento de texto y medio electrónico	Informe contenido dentro de la actuación procesal
INFORMES DE APOYO TÉCNICO	No	Si	Informes de apoyo ténico	Apoyo ténico dentro de las actuaciones procesales	Español	Físico y electrónico	Documento de texto y medio electrónico	Informe contenido dentro de la actuación procesal
INFORMES DE GESTIÓN	No	Si	Informes de gestión	Información detallada sobre actividad desarrollada por la segunda instancia y su avance	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo de la Dirección de Juicios Fiscales
NOTIFICACIONES POR ESTADO	No	Si	Notificaciones por estado	Publicación del respectivo acto administrativo según Artículo 106 Ley 1474 de 2011	Español	Físico y electrónico	Documento de texto y medio electrónico	Secretaría Común Conjunta adscrita al Despacho de la Delegada para Investigaciones
OFICIOS DE CITACIONES	No	Si	Oficios de citaciones	Se emite por los Abogados Sustanciadores o por la Secretaría Común Conjunta. En este último caso, por desconocimiento del domicilio del por notificar	Español	Físico y electrónico	Documento de texto y medio electrónico	Secretaría Común Conjunta adscrita al Despacho de la Delegada para Investigaciones o el Despacho mismo
PROCESOS DE RESPONSABILIDAD FISCAL	No	Si	Procesos de responsabilidad fiscal	Resolver la segunda instancia y el grado de consulta del Proceso de Responsabilidad Fiscal y ocasionalmente llevar la Investigación dirigida a probar la existencia o no de daño fiscal y su cuantificación, producido por dolo o culpa de	Español	Físico y electrónico	Documento de texto y medio electrónico	Archivo del Despacho de la Dirección de Juicios Fiscales
NOTIFICACION POR PAG WEB	Si	Notificación	Notificación de Providencias	Forma de dar a conocer una decisión dentro de un proceso a las partes y sus apoderados	Español	Físico y Electrónico	Documento texto	Página Web http://www.Gerenteia.gov.co/ Link Notificaciones - Jurisdicción Coactiva
ACTUACIONES ESPECIALES DE CONTROL FISCAL	Se encuentra disponibl	Se encuentra disponible el informe final en la página	Actuaciones Especiales	Son acciones de fiscalización que se caracterizan por ser breves y sumarias, en las que un funcionario o equipo de trabajo aborda la investigación de un hecho o un asunto que llegue al conocimiento de la Gerenteía General de la República, por cualquier medio de información o denuncia ciudadana, que	Español	Electrónico	PDF Digital	El informe final en la página Web de la Gerenteia General de la República, una vez terminado la actuación especial
CONTROL EXCEPCIONAL	Se encuentra	Se encuentra disponible el informe	Control excepcional	El control excepcional son auditoría realizada a entes territoriales y se justifica cuando se coloca en duda la imparcialidad del órgano territorial de control, debido a presiones o injerencias locales	Español	Electrónico	PDF Digital	El informe final en la página Web de la Gerenteia General de la República, una vez terminado el Control Excepcional

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS								Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
AUDITORÍA	Se encuentra disponible el informe	Se encuentra disponible el informe final en la página Web	Auditoría	Es un proceso sistemático que evalúa, acorde con las normas de auditoría generalmente aceptadas vigentes, la política pública y/o la gestión y los resultados fiscales de los entes objeto de control fiscal y de los planes, programas, proyectos y/o asuntos a auditar, mediante la aplicación de los sistemas de control fiscal o actuaciones especiales de vigilancia y control, para determinar el cumplimiento de los principios de la gestión fiscal.	Español	Electrónico	PDF Digital	El informe final en la página Web de la Gerenteia General de la República, una vez terminado la auditoría
PROCESOS (Administrativos sancionatorios)	Se encuentra disponible en el archivo de gesti	Se encuentra disponible en el archivo de gestión de la Delegada solo en cuando se tenga la resolución	Procesos (Administrativos sancionatorios)	El procesos sancionatorios contra orientados a establecer si la acción u omisión del particular ha infringido la normatividad que la regula y en consecuencia determinar si es procedente o no imponer las sanciones contempladas para la respectiva infracción	Español	Papel	Documento texto	Se encuentra en el Archivo de Gestión de la Gerenteía Delegada para el Sector Agropecuario disponible solo hasta enero de 2016
RELACIONES TÉCNICAS CON EL CONGRESO	Se encuentra disponible en	Se encuentra disponible en el Archivo de Gestión de la	Relaciones técnicas con el Congreso	Prestar Asistencia Técnica al Congreso de la República, a través del trámite oportuno y respuestas integrales a sus solicitudes, así como el seguimiento a proyectos de ley y de acto legislativo	Español	Papel	Documento texto	Archivo de Gestión de la Gerenteía Delegada para el Sector Agropecuario a enero 2016
RESOLUCIONES (Audiencias Publicas, sancionatorias)	Se encuentra disponible en	Se encuentra disponible en el Archivo de Gestión de la	Resoluciones (Sancionatorias)	Fallo de una autoridad	Español	Papel	Documento texto	Archivo de Gestión de la Gerenteía Delegada para el Sector Agropecuario a enero 2016
SUPERVISIÓN DE CONTRATOS	Se encuentra disponible en	Se encuentra disponible en el Archivo de Gestión de la	Supervisión de contratos	Consiste en el seguimiento técnico, administrativo, financiero, contable y jurídico que sobre el cumplimiento del objeto del contrato	Español	Papel	Documento texto	Archivo de Gestión de la Gerenteía Delegada para el Sector Agropecuario a enero 2016
URGENCIA MANIFIESTA	Se encuentra disponible en	Se encuentra disponible en el Archivo de Gestión de la	Urgencia manifiesta	Autorización al jefe o representante legal de la respectiva entidad estatal, para hacer la declaración de urgencia con el carácter de manifiesta, cuando se presenten situaciones excepcionales relacionadas con calamidades, desastres, fuerza mayor, guerra exterior o conmoción interior, emergencia económica, social	Español	Papel	Documento texto	Archivo de Gestión de la Gerenteía Delegada para el Sector Agropecuario a enero 2016
ACTUACIONES ESPECIALES DE CONTROL FISCAL	Se encuentra disponible	Se encuentra disponible el informe final en la página	Actuaciones especiales	Son acciones de fiscalización que se caracterizan por ser breves y sumarias, en las que un funcionario o equipo de trabajo aborda la investigación de un hecho o un asunto que llegue al conocimiento de la Gerenteía General de la República, por cualquier medio de información o denuncia ciudadana, que	Español	Electrónico	PDF Digital	El informe final en la página Web de la Gerenteia General de la República, una vez terminado la actuación especial
AUDITORÍA	Se encuentra disponible el	Se encuentra disponible el informe final en la página Web	Auditoría	Es un proceso sistemático que evalúa, acorde con las normas de auditoría generalmente aceptadas vigentes, la política pública y/o la gestión y los resultados fiscales de los entes objeto de control fiscal y de los planes, programas, proyectos y/o asuntos a auditar, mediante la aplicación de los sistemas de control fiscal o actuaciones especiales de vigilancia y control, para determinar el cumplimiento de los principios de la gestión fiscal.	Español	Electrónico	PDF Digital	El informe final en la página Web de la Gerenteia General de la República, una vez terminado la auditoría

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS								Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
BENEFICIOS DEL PROCESO AUDITOR	Se encuentra disponible en el	Se encuentra disponible en el Archivo de Gestión de la Gerenteia	Beneficios del proceso auditor	El reporte de beneficios del control fiscal es una forma de medir el impacto del proceso auditor que desarrolla laINSTITUTO NACIONAL DE MUSEOS(CGR); por lo tanto se deberá cuantificar o cualificar el valor agregado generado por el ejercicio del control fiscal, bien se trate de acciones evidenciadas, que correspondan al seguimiento de acciones establecidas en planes de mejoramiento o	Español	Papel	Documento de texto	Archivo de Gestion de la Gerenteia Delegada para el Sector Agropecuario a enero 2016
INDAGACIONES PRELIMINARES	Se encuentra disponible en el Archivo de Gesti	Se encuentra disponible en el Archivo de Gestion de la Gerenteia Delegada para el Sector Agropecua	Indagaciones Preliminares	Procedimiento que se caracteriza por ser extraprocesal, y se debe surtir cuando se dificulta la configuración de un hallazgo fiscal perfecto	Español	Electrónico y Papel	Documento de texto	Solo se encuentra disponible para funcionarios de laINSTITUTO NACIONAL DE MUSEOSen SAE y SIREF
INFORMES	Se encuentra	Se encuentra disponible el informe	Informe de auditoria	Es el documento que sintetiza el resultado del cumplimiento de los objetivos definidos en la asignación de actividades de auditoría, en el plan de trabajo y el resultado de las pruebas	Español	Electrónico y Papel	PDF Digital	Se encuentra disponible el informe final en la página Web
URGENCIA MANIFIESTA	Se encuentra disponible en	Se encuentra disponible en el Archivo de Gestion de la	Urgencia manifiesta	Autorización al jefe o representante legal de la respectiva entidad estatal, para hacer la declaración de urgencia con el carácter de manifiesta, cuando se presenten situaciones excepcionales relacionadas con calamidades, desastres, fuerza mayor, guerra exterior o conmoción interior, emergencia económica, social	Español	Papel	Documento de texto	Archivo de Gestion de la Gerenteia Delegada para el Sector Agropecuario a enero 2016
FUNCIÓN DE ADVERTENCIA	Se encuentra disponible en el Archivo de Gestion	Se encuentra disponible en el Archivo de Gestion de la Gerenteia Delegada para el Sector Agropecuario. Solo	Función de advertencia	Es un instrumento de carácter técnico preventivo y proactivo, que no puede entenderse como un sistema de control fiscal, toda vez que su fin no es otro, que señalar a la entidad fiscalizada la existencia de situaciones o hechos que no ofrecen confianza en su realización y por tanto ameritan la revisión por parte de la administración a fin de evitar un posible daño al Erario Público, sin perjuicio del ejercicio de la vigilancia y control fiscal posterior atribuida a la Gerenteia, sobre los hechos así identificados, momento en el cual se concreta y evidencia la efectividad de esta especial atribución. Solo estan los pronuciamiento hasta el 2014, fue	Español	Físico	Físico y Digital	Solo se encuentra disponible para funcionarios de la Gerenteia Genenral de la República en SIIGEP, solo las anteriores al 2014
APOYO AL PROCESO AUDITOR - DIAGNOSTICOS SECTORIALES	Diagnósticos sectoriales	Se encuentra disponible en el Archivo de Gestion de	Apoyo al proceso auditor	Insumo para la elaboración de los Planes del Control Fiscal	Español	Documento texto - Digital	Documento de texto	Se encuentra disponible en el Archivo de Gestion de la Gerenteia Delegada para el Sector Agropecuario
APOYO AL PROCESO AUDITOR - DIAGNOSTICOS SECTORIALES	Documentos técni	Hace parte de los informes finales de	Apoyo al proceso auditor	Documentos sobre aspectos para el desarrollo de las auditorias	Español	Documento texto - Digital	Documento de texto	Hace parte de los informes finales de auditoria
ESTUDIOS E INVESTIGACIONES	Análisis sectorial y de políti	Se encuentra disponible en el Archivo de Gestion de	Estudios e Investigaciones	Corresponde a análisis y evaluaciones de las políticas públicas del PND o de políticas de interés para laINSTITUTO NACIONAL DE MUSEOS	Español	Documento texto - Digital Algunos se públican	Documento de texto	Se encuentra disponible en el Archivo de Gestion de la Gerenteia Delegada para el Sector Agropecuario
ESTUDIOS E INVESTIGACIONES	Análisis de proyectos de	Se encuentra disponible en el Archivo de Gestion de	Estudios e Investigaciones	Se refieren a la revisión de los proyectos de ley de la agenda de interés para laINSTITUTO NACIONAL DE MUSEOS	Español	Documento texto - Digital	Documento de texto	Se encuentra disponible en el Archivo de Gestion de la Gerenteia Delegada para el Sector Agropecuario
REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS								Versión 1.0

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS								Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SFR	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
ESTUDIOS E INVESTIGACIONES	Artículos, revistas y publicacio	Se encuentra disponible en el Archivo de Gestion de	Estudios e Investigaciones	Son síntesis de las evaluaciones de política o de temas de interés para laINSTITUTO NACIONAL DE MUSEOS	Español	Documento texto - Digital	Documento de texto	Se encuentra disponible en el Archivo de Gestion de la Gerenteia Delegada para el Sector Agropecuario
ESTUDIOS E INVESTIGACIONES	Participación en actividad	Se encuentra disponible en el Archivo de Gestion de	Estudios e Investigaciones	Son documentos de apoyo para la realización o participación en actividades académicas relacionadas con las políticas sectoriales	Español	Documento texto - Digital	Documento de texto	Se encuentra disponible en el Archivo de Gestion de la Gerenteia Delegada para el Sector Agropecuario
ESTUDIOS E INVESTIGACIONES	Participación en estudios	Se encuentra disponible en el Archivo de Gestion de	Estudios e Investigaciones	Se refiere a los documentos elaborados a partir de la participación en las evaluaciones macroeconomías, coordinadas por la Gerenteia Delegada de Economía y Finanzas Públicas	Español	Documento texto - Digital	Documento de texto	Se encuentra disponible en el Archivo de Gestion de la Gerenteia Delegada para el Sector Agropecuario
INFORMES	Informes de apoyo técni	Se encuentra disponible en el Archivo de Gestion de	Informes	Documentos técnicos sobre aspectos del sector	Español	Documento texto - Digital	Documento de texto	Se encuentra disponible en el Archivo de Gestion de la Gerenteia Delegada para el Sector Agropecuario
INFORMES	Informes de gestión	Se encuentra disponible en el Archivo de Gestion de	Informes	Presentación de las actividades realizadas por la Dirección de Estudios Sectoriales de la Gerenteia Delegada para el Sector Agropecuario	Español	Documento texto - Digital	Documento de texto	Se encuentra disponible en el Archivo de Gestion de la Gerenteia Delegada para el Sector Agropecuario
INFORMES	Informes sectoriales al Cong	Se encuentra disponible en el Archivo de Gestion de	Informes	Resultados de la evaluación sectorial de la gestión ambiental de las entidades del sector	Español	Documento texto - Digital	Documento de texto	Se encuentra disponible en el Archivo de Gestion de la Gerenteia Delegada para el Sector Agropecuario
INFORMES	Informes sectoriales sobre la	Se encuentra disponible en el Archivo de Gestion de	Informes	Resultados de la evaluación sectorial del sistema de control interno de las entiddaes en el sector	Español	Documento texto - Digital	Documento de texto	Se encuentra disponible en el Archivo de Gestion de la Gerenteia Delegada para el Sector Agropecuario
ACTAS (COMITÉ DE EVALUACION SECTORIAL, COMITÉ TÉCNICO)	NO	NO	Actas (Comité de evaluación sectorial, comité técnico)		Español	Fisico		Archivo de Gestión de la Gerenteía Delegada para el Sector Social
ACTUACIONES ESPECIALES DE CONTROL FISCAL	SÍ	SÍ			Español	Fisico y Electrónico	Papel y Documento electrónico	Archivo de Gestión de la Gerenteía Delegada para el Sector Social
ADJUDICACIÓN DE LICITACIÓN EN AUDIENCIA PÚBLICA	No aplica	No aplica			Español	No aplica	No aplica	No aplica
ANTECEDENTES FISCALES	No aplica				Español	No aplica	No aplica	No aplica
CONCEPTOS JURIDICOS	No aplica	No aplica			Español	Fisico	No aplica	No aplica
CONTROL EXCEPCIONAL	SÍ	SÍ			Español	Fisico y Electrónico	Papel y Documento electrónico	Archivo de Gestión de la Gerenteía Delegada para el Sector Social
DOCUMENTOS DE ORIGEN CIUDADANO (Acciones Populares-Denuncias-Derechos de Petición- Tutelas)	NO	SI			Español	Fisico y Electrónico	Papel y Documento electrónico	Archivo de Gestión de la Gerenteía Delegada para el Sector Social

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS								Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
FUNCIÓN DE ADVERTENCIA	No aplica	No aplica			Español	Fisico y Electrónico	Papel y Documento electrónico	Archivo de Gestión de la Gerenteía Delegada para el Sector Social
INFORMES FINALES (Auditoria-SGPP Informes Congreso	SÍ	SÍ			Español	Fisico y Electrónico	Papel y Documento electrónico	Archivo de Gestión de la Gerenteía Delegada para el Sector Social
PROCESOS (Administrativos sancionatorios)	NO	NO			Español	Fisico	Papel	Archivo de Gestión de la Gerenteía Delegada para el Sector Social
RELACIONES TÉCNICAS CON EL CONGRESO	NO	SÍ			Español	Fisico		Archivo de Gestión de la Gerenteía Delegada para el Sector Social
RESOLUCIONES (Audiencias Publicas, sancionatorias)	NO	SÍ			Español	Fisico		Archivo de Gestión de la Gerenteía Delegada para el Sector Social
SOLICITUDES DE AJUSTES AL PLAN GENERAL DE AUDITORÍA	NO	SÍ			Español	Fisico		Archivo de Gestión de la Gerenteía Delegada para el Sector Social
TRASLADO DE HALLAZGOS FISCALES, DISCIPLINARIOS Y PENALES	NO	SÍ			Español	Fisico		Archivo de Gestión de la Gerenteía Delegada para el Sector Social
URGENCIA MANIFIESTA	SÍ	SÍ			Español	Fisico		Archivo de Gestión de la Gerenteía Delegada para el Sector Social
ACTAS (ACTAS DE SEGUIMIENTO AL PLAN GENERAL DE AUDITORIA - PGA	NO	NO	Actas seguimiento - PGA	Seguimiento	Español	Fisico	Papel	Archivo de Gestión de la Gerenteía Delegada para el Sector Social
ACTUACIONES ESPECIALES DE CONTROL FISCAL	SÍ	SÍ			Español	Fisico	Papel	Archivo de Gestión de la Gerenteía Delegada para el Sector Social
ANTECEDENTES FISCALES	No aplica	No aplica			Español	Fisico	Papel	Archivo de Gestión de la Gerenteía Delegada para el Sector Social
AUDITORÍA	SÍ	SÍ			Español	Fisico y Electrónico SICA	Papel - Electrónico	Archivo de Gestión de la Gerenteía Delegada para el Sector Social
BENEFICIOS DEL PROCESO AUDITOR	SÍ	SÍ			Español	Fisico	Papel	Archivo de Gestión de la Gerenteía Delegada para el Sector Social
CUENTAS E INFORMES CONSOLIDADOS DE LOS SUJETOS DE CONTROL	SÍ	SÍ			Español	Electrónico - SIRECI	Papel - Electrónico SIRECI	Archivo de Gestión de la Gerenteía Delegada para el Sector Social
DOCUMENTO DE ORIGEN CIUDADANO(Denuncias-Derechos de Petición	NO	SI			Español	Fisico y Electrónico	Papel - Documento Electrónico	Archivo de Gestión de la Gerenteía Delegada para el Sector Social
INDAGACIONES PRELIMINARES	NO	NO			Español	Fisico	Papel	Archivo de Gestión de la Gerenteía Delegada para el Sector Social
INFORMES (Apoyo Técnico, Austeridad del Gasto,Auditoría del Balance de la Nación,Culminación de Gestión,Deuda Servicios Públicos, Informes Gestión,Planes Mejoramiento, Plan de Gestión información estrátegica	SÍ	SÍ			Español	Fisico	Papel - Electrónico	Archivo de Gestión de la Gerenteía Delegada para el Sector Social
REPORTES DE OBSERVATORIO (Documentos Electrónicos)	No aplica	No aplica			Español	Fisico	Papel	Archivo de Gestión de la Gerenteía Delegada para el Sector Social
TRASLADO DE HALLAZGOS FISCALES, DISCIPLINARIOS Y PENALES	SÍ	SÍ			Español	Fisico	Papel	Archivo de Gestión de la Gerenteía Delegada para el Sector Social

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS								Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
ACTUACIONES ESPECIALES DE CONTROL FISCAL	SÍ	SÍ			Español	Fisico	Papel	Archivo de Gestión de la Gerenteía Delegada para el Sector Social
ANTECEDENTES FISCALES	No aplica	No aplica			Español	Fisico	Papel	No aplica
APOYO AL PROCESO AUDITOR - DIAGNOSTICOS SECTORIALES	SÍ	SÍ			Español	Fisico	Papel	Archivo de Gestión de la Gerenteía Delegada para el Sector Social
ESTUDIOS E INVESTIGACIONES	SÍ	SÍ			Español	Fisico	Papel	Archivo de Gestión de la Gerenteía Delegada para el Sector Social
FUNCIÓN DE ADVERTENCIA	No aplica	No aplica			Español	Fisico	Papel	No aplica
INFORMES	SÍ	SÍ			Español	Fisico	Papel	Archivo de Gestión de la Gerenteía Delegada para el Sector Social
MATRIZ DE RIESGO DE SUJETOS DE CONTROL	SÍ	SÍ			Español	Fisico	Papel	Archivo de Gestión de la Gerenteía Delegada para el Sector Social
ACTAS (COMITÉ DE EVALUACION SECTORIAL, COMITÉ TÉCNICO)	NO	NO	Actas (Comité de evaluación sectorial, comité técnico)	No aplica	Español	Físico y electrónico	Papel y documento electrónico	Archivo de Gestión de la Gerenteía Delegada para el Sector Infraestructura Física y Telecomunicaciones, Comercio Exterior y Desarrollo Regional
ACTUACIONES ESPECIALES DE CONTROL FISCAL	SÍ	SÍ	Actuaciones especiales de control fiscal	No aplica	Español	Físico y electrónico	Papel y documento electrónico	Archivo de Gestión de la Gerenteía Delegada para el Sector Infraestructura Física y Telecomunicaciones, Comercio Exterior y Desarrollo Regional
ADJUDICACIÓN DE LICITACIÓN EN AUDIENCIA PÚBLICA	NO	NO	Adjudicación de licitación en audiencia pública	No aplica	Español	No aplica	No aplica	No aplica
ANTECEDENTES FISCALES	No hay prod		Antecedentes fiscales	No aplica	Español	No aplica	No aplica	No aplica
CONCEPTOS JURIDICOS	NO	SÍ	Conceptos jurídicos	Conceptos jurídicos	Español	Físico y electrónico	Papel y documento electrónico	Archivo de Gestión de la Gerenteía Delegada para el Sector Infraestructura Física y Telecomunicaciones, Comercio Exterior y Desarrollo Regional
CONTROL EXCEPCIONAL	SÍ	SÍ	Control excepcional	Control excepcional	Español	Físico y electrónico	Papel y documento electrónico	Archivo de Gestión de la Gerenteía Delegada para el Sector Infraestructura Física y Telecomunicaciones, Comercio Exterior y Desarrollo Regional
FUNCIÓN DE ADVERTENCIA	NO	NO	Función de advertencia	No aplica	Español	No aplica	Papel y documento electrónico	No aplica
INDAGACIONES PRELIMINARES	NO	NO	Indagaciones preliminares	No aplica	Español	Físico y electrónico	Papel y documento electrónico	Archivo de Gestión de la Gerenteía Delegada para el Sector Infraestructura Física y Telecomunicaciones, Comercio Exterior y Desarrollo Regional
INFORMES (Auditoria, congreso)	SÍ	SÍ	Informes (Auditoria, congreso)	Informes	Español	Físico y electrónico	Papel y documento electrónico	Archivo de Gestión de la Gerenteía Delegada para el Sector Infraestructura Física y Telecomunicaciones, Comercio Exterior y Desarrollo Regional
PROCESOS (Administrativos sancionatorios)	NO	SÍ	Procesos (Administrativos sancionatorios)	Procesos (Administrativos sancionatorios)	Español	Físico y electrónico	Papel y documento electrónico	Archivo de Gestión de la Gerenteía Delegada para el Sector Infraestructura Física y Telecomunicaciones, Comercio Exterior y Desarrollo Regional

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS								Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SFR	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
RELACIONES TÉCNICAS CON EL CONGRESO	NO	SÍ	Relaciones técnicas con el Congreso	Relaciones técnicas con el Congreso	Español	Físico y electrónico	Papel y documento electrónico	Archivo de Gestión de la Gerenteía Delegada para el Sector Infraestructura Física y Telecomunicaciones, Comercio Exterior y Desarrollo Regional
RESOLUCIONES (Audiencias Publicas, sancionatorias)	NO	SÍ	Resoluciones (Audiencias Publicas, sancionatorias)	Resoluciones (Audiencias Publicas, sancionatorias)	Español	Físico	Papel	Archivo de Gestión de la Gerenteía Delegada para el Sector Infraestructura Física y Telecomunicaciones, Comercio Exterior y Desarrollo Regional
SOLICITUDES DE AJUSTES AL PLAN GENERAL DE AUDITORÍA	NO	SÍ	Solicitudes de ajustes al Plan General de Auditoría	Solicitudes de ajustes al Plan General de Auditoría	Español	Físico y electrónico	Papel y documento electrónico	Archivo de Gestión de la Gerenteía Delegada para el Sector Infraestructura Física y Telecomunicaciones, Comercio Exterior y Desarrollo Regional
TRASLADO DE HALLAZGOS FISCALES, DISCIPLINARIOS Y PENALES	NO	SÍ	Traslado de hallazgos fiscales, disciplinarios y penales	Traslado de hallazgos fiscales, disciplinarios y penales	Español	Físico y electrónico	Papel y documento electrónico	Archivo de Gestión de la Gerenteía Delegada para el Sector Infraestructura Física y Telecomunicaciones, Comercio Exterior y Desarrollo Regional
URGENCIA MANIFIESTA	SÍ	SÍ	Urgencia manifiesta	Urgencia manifiesta	Español	Físico y electrónico	Papel y documento electrónico	Archivo de Gestión de la Gerenteía Delegada para el Sector Infraestructura Física y Telecomunicaciones, Comercio Exterior y Desarrollo Regional
ACTAS (ACTAS DE SEGUIMIENTO AL PLAN GENERAL DE AUDITORIA - PGA)	SÍ	SÍ	Actas (Actas de seguimiento al Plan General de Auditoria - PGA)	Actas de comité técnico en sus diferentes etapas del PGA.	Español	Electronico y Papel	Físico y digital	Papeles de trabajo.
ACTUACIONES ESPECIALES DE CONTROL FISCAL	SÍ	SÍ	Actuaciones especiales de control fiscal	Son acciones de fiscalización que se caracterizan por ser breves y sumarias, en las que un funcionario o equipo de trabajo aborda la investigación de un hecho o un asunto que llegue al conocimiento de la Gerenteía General de la República, por cualquier medio de información o denuncia ciudadana, que	Español	Electronico y Papel	Fisico y digital	Solo se encuentra disponible el informe final en la pagina Web
ANTECEDENTES FISCALES	SÍ	SÍ	Antecedentes fiscales	Es un hallazgo trasladado al grupo IP de auditoria es un hecho relevante que se constituye en un resultado determinante en la evaluación de un asunto en particular, al comparar la condición [situación detectada] con el criterio [deber ser]. Igualmente, es una situación determinada al aplicar	Español	Electronico y Papel	Físico y digital	En SAE para las partes procesales y SIREF solo se encuentra disponible para funcionarios de la CGR
AUDITORÍA	SÍ	SÍ	Auditoría	Es un proceso sistemático que evalúa, acorde con las normas de auditoría generalmente aceptadas vigentes, la política pública y/o la gestión y los resultados fiscales de los entes objeto de control fiscal y de los planes, programas, proyectos y/o asuntos a auditar, mediante la aplicación de los sistemas de control fiscal o actuaciones especiales de vigilancia y control, para determinar el cumplimiento de los principios de la gestión fiscal	Español	Electronico y Papel	Físico y digital	Solo se encuentra disponible el informe final en la pagina Web
BENEFICIOS DEL PROCESO AUDITOR	SÍ	SÍ	Beneficios del proceso auditor	El reporte de beneficios del control fiscal es una forma de medir el impacto del proceso auditor que desarrolla laINSTITUTO NACIONAL DE MUSEOS(CGR); por lo tanto se deberá cuantificar o cualificar el valor agregado generado por el ejercicio del control fiscal, bien se trate de acciones evidenciadas, que correspondan al seguimiento de acciones establecidas en planes de mejoramiento o	Español	Electronico y Papel	Físico y digital	Solo se encuentra disponible para funcionarios de la CGR en SIIGEP
CUENTAS E INFORMES CONSOLIDADOS DE LOS SUJETOS DE CONTROL	SÍ	SÍ	Cuentas e informes consolidados de los sujetos de control	Información que se debe presentar a laINSTITUTO NACIONAL DE MUSEOSsobre las actuaciones legales, técnicas, contables, financieras y de gestión, como resultado de la administración.	Español	Electronico y Papel	Digital	Solo se encuentra disponible para funcionarios de la CGR en SIRECI
FUNCIÓN DE ADVERTENCIA	NO	NO	Función de advertencia	No aplica	Español	No aplica	No aplica	No aplica
INDAGACIONES PRELIMINARES	SÍ	SÍ	Indagaciones preliminares	Procedimiento que se caracteriza por ser extraprocesal, y se debe surtir cuando se dificulta la configuración de un hallazgo fiscal perfecto	Español	Electronico y Papel	Físico y Digital	Solo se encuentra disponible para funcionarios de la CGR en SAE y SIREF

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS								Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
INFORMES SOBRE GESTIÓN FISCAL	NO	Mediante Aplicativo SICA	Informes sobre gestión fiscal	Mecanismo mediante el cual se ejerce especial seguimiento, control y vigilancia de los recursos que involucren grandes cantidades de dinero o causen impacto nacional	Español	Físico – Electrónico	Papel generalmente carta y oficio. Electronicos (Magneticos) contenidos en CD: Archivos en formato MS excel.xls y PDF.	Archivo de Gestión de la Gerenteía Delegada para el Sector de Minas y Energía - Aplicativo SICA
INFORMES DE ESPECIAL SEGUIMIENTO	NO	Mediante Aplicativo SICA	Informes de especial seguimiento	Mecanismo mediante el cual se ejerce especial seguimiento, control y vigilancia de los recursos que involucren grandes cantidades de dinero o causen impacto nacional	Español	Físico – Electrónico	Papel generalmente carta y oficio. Electronicos (Magneticos) contenidos en CD: Archivos en formato MS excel.xls y PDF.	Archivo de Gestión de la Gerenteía Delegada para el Sector de Minas y Energía - Aplicativo SICA
INFORMES DE OBSERVATORIOS	NO	Mediante Aplicativo SICA	Informes de observatorios	Mecanismo mediante el cual se ejerce especial seguimiento, control y vigilancia de los recursos que involucren grandes cantidades de dinero o causen impacto nacional	Español	Físico – Electrónico	Papel generalmente carta y oficio. Electronicos (Magneticos) contenidos en CD: Archivos en formato MS excel.xls y PDF.	Archivo de Gestión de la Gerenteía Delegada para el Sector de Minas y Energía - Aplicativo SICA
ACTUACIONES ESPECIALES DE FISCALIZACIÓN	NO	Mediante Aplicativo SICA	Actuaciones especiales de fiscalización	Mecanismo mediante el cual se ejerce especial seguimiento, control y vigilancia de los recursos que involucren grandes cantidades de dinero o causen impacto nacional	Español	Físico – Electrónico	Papel generalmente carta y oficio. Electronicos (Magneticos) contenidos en CD: Archivos en formato MS excel.xls y PDF.	Archivo de Gestión de la Gerenteía Delegada para el Sector de Minas y Energía - Aplicativo SICA
INFORMES DE SEGUIMIENTO A LOS PLANES DE DESARROLLO	NO	Mediante Aplicativo SICA	Informes de seguimiento a los planes de desarrollo	Mecanismo mediante el cual se ejerce especial seguimiento, control y vigilancia de los recursos que involucren grandes cantidades de dinero o causen impacto nacional	Español	Físico – Electrónico	Papel generalmente carta y oficio. Electronicos (Magneticos) contenidos en CD: Archivos en formato MS excel.xls y PDF.	Archivo de Gestión de la Gerenteía Delegada para el Sector de Minas y Energía - Aplicativo SICA
INFORMES DE ANÁLISIS SISTÉMICO A LA ADMINISTRACIÓN PÚBLICA	NO	Mediante Aplicativo SICA	Informes de análisis sistémico a la administración pública	Mecanismo mediante el cual se ejerce especial seguimiento, control y vigilancia de los recursos que involucren grandes cantidades de dinero o causen impacto nacional	Español	Físico – Electrónico	Papel generalmente carta y oficio. Electronicos (Magneticos) contenidos en CD: Archivos en formato MS excel.xls y PDF.	Archivo de Gestión de la Gerenteía Delegada para el Sector de Minas y Energía - Aplicativo SICA

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS								Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
AUDITORIA	SI	Mediante Aplicativo SICA	Auditoría	Un proceso sistemático que evalua, acorde con las normas de auditoría generalmente aceptadas vigentes, la política pública y/o la gestión y los resultados fiscales de los entes objeto de control fiscal y de los planes, programas, proyectos y/o asuntos a auditar, mediante la aplicación de los sistemas de control fiscal o actuaciones especiales de vigilancia y control, para determinar el cumplimiento de los principios de la gestión fiscal, en la prestación de servicios o provisión de bienes	Español	Físico – Electrónico	Papel generalmente carta y oficio. Electronicos (Magneticos) contenidos en CD: Archivos en formato MS excel.xls y PDF.	Archivo de Gestión de la Gerenteía Delegada para el Sector de Minas y Energía - Aplicativo SICA
BENEFICIOS DEL PROCESO AUDITOR	SI	Mediante Aplicativo SIIGEP	Beneficios del proceso auditor	Forma de medir el impacto del proceso auditor; cuantifica o cualifica el valor agregado generado por el ejercicio del control fiscal, bien se trate de acciones evidenciadas, que correspondan al seguimiento de acciones establecidas en planes de mejoramiento o que sean producto de observaciones, hallazgos, pronunciamientos o advertencias efectuados por la CGR y que exista una relación directa entre la acción de mejoramiento y el beneficio	Español	Físico – Electrónico	Papel generalmente carta y oficio. Electronicos (Magneticos) contenidos en CD: Archivos en formato MS excel.xls y PDF.	Archivo de Gestión de la Gerenteía Delegada para el Sector de Minas y Energía - Aplicativo SIRECI
COMUNICACIONES INFORMATIVAS	NO	Se encuentran copias de las comunicaciones enviadas y recibidas por el despacho	Comunicaciones informativas	Son Las comunicaciones oficiales de caracter informativo enviadas y recibidas en soporte papel	Español	Físico – Electrónico	Papel generalmente carta y oficio. Electronicos (Magneticos) contenidos en CD: Archivos en formato MS excel.xls y PDF.	Archivo de Gestión de la Gerenteía Delegada para el Sector de Minas y Energía - Aplicativo SIGEDOC
CONTROL EXCEPCIONAL	NO	NO	Control excepcional	Facultad para ejercer control fiscal posterior sobre cuentas de cualquier entidad territorial	Español	Físico – Electrónico	Papel generalmente carta y oficio. Electronicos (Magneticos) contenidos en CD: Archivos en formato MS excel.xls y PDF.	Archivo de Gestión de la Gerenteía Delegada para el Sector de Minas y Energía - Aplicativo SICA
DOCUMENTOS DE ORIGEN CIUDADANO	SI	Mediante aplicativo SIPAR	Documentos de origen ciudadano	Documentos relacionadas con denuncias, derechos de petición, acciones populares, tutelas y otras solicitudes	Español	Físico – Electrónico	Papel generalmente carta y oficio. Electronicos (Magneticos) contenidos en CD: Archivos en formato MS excel.xls y PDF.	Archivo de Gestión de la Gerenteía Delegada para el Sector de Minas y Energía - Aplicativo SIPAR
INDAGACIONES PRELIMINARES	NO	Mediante aplicativo SIREF	Indagaciones preliminares	Función de investigación o indagación que se requiera, por hechos relacionados contra los intereses patrimoniales del Estado y que comprometan recursos del mismo	Español	Físico – Electrónico	Papel generalmente carta y oficio. Electronicos (Magneticos) contenidos en CD: Archivos en formato MS excel.xls y PDF.	Archivo de Gestión de la Gerenteía Delegada para el Sector de Minas y Energía - Aplicativo SIREF

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS									Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
INFORME FINAL DE AUDITORIA	SI	Página Web y documento físico	Informe final de auditoria	Documento mediante el cual se reporta la evaluación y/o gestión que se haya generado sobre diferentes procesos que se realizan dentro de la entidad conforme la ley	Español	Físico – Electrónico	Papel generalmente carta y oficio. Electronicos (Magneticos) contenidos en CD: Archivos en formato MS excel.xls y PDF.	Archivo de Gestión de la Gerenteía Delegada para el Sector de Minas y Energía - Página Web
INFORMES DE GESTIÓN	NO	NO	INFORMES DE GESTIÓN	Documento mediante el cual se reporta la evaluación y/o gestión que se haya generado sobre diferentes procesos que se realizan dentro de la entidad conforme la ley.	Español	Físico – Electrónico	Papel generalmente carta y oficio. Electronicos (Magneticos) contenidos en CD: Archivos en formato MS excel.xls y PDF.	Archivo de Gestión de la Gerenteía Delegada para el Sector de Minas y Energía - Aplicativo SICA
PROCESOS ADMINISTRATIVOS SANCIONATORIOS	NO	SI	Procesos Administrativos Sancionatorios	Proceso mediante el cual se ejerce la potestad sancionadora	Español	Físico – Electrónico	Papel generalmente carta y oficio. Electronicos (Magneticos) contenidos en CD: Archivos en formato MS excel.xls y PDF.	Archivo de Gestión de la Gerenteía Delegada para el Sector de Minas y Energía - Aplicativo SICA
ESTUDIOS E INVESTIGACIONES	NO	SI	Estudios e investigaciones	Investigación que evalúa el impacto de una política pública en términos de eficiencia y eficacia y no solo muestra los resultados alcanzados	Español	Físico – Electrónico	Papel generalmente carta y oficio. Electronicos (Magneticos) contenidos en CD: Archivos en formato MS excel.xls y PDF.	Archivo de Gestión de la Gerenteía Delegada para el Sector de Minas y Energía - Pagina Web
ACTAS (COMITÉ DE EVALUACION SECTORIAL, COMITÉ TÉCNICO)	Actas	SI	Actas de comité técnico	Actas de comité Técnico	Español	Fisico	Documento texto	Archivo de Gestión de la Gerenteía Delegada para el Medio Ambiente
ACTAS AL CULMINAR LA GESTIÓN	Actas Culm	SI	Actas Culminación de la Gestión	Actas Culminación de la Gestión	Español	Fisico	Documento texto	Archivo de Gestión de la Gerenteía Delegada para el Medio Ambiente
ACTAS DE ENTREGA DE DEPENDENCIA	Actas	SI	Actas de entrega de dependencia	Actas de entrega de dependencia ya sea por nombramiento o por finalización del periodo	Español	Fisico	Documento texto	Archivo de Gestión de la Gerenteía Delegada para el Medio Ambiente
ACTUACIONES ESPECIALES DE CONTROL FISCAL	Informes	SI	Actuaciones Especiales de Control Fiscal	Informes de Auditoria con tematica especifica: Gestión Fiscal, de seguimiento, de Observatorios, de consultas de información, de fiscalización entre	Español	Fisico - Digital	Documento texto - Digital-SICA	Archivo de Gestión de la Gerenteía Delegada para el Medio Ambiente
PROCESOS (Administrativos sancionatorios)	Resolución	SI	Procesos administrativos sancionatorios	Proceso sancionatorio	Español	Fisico-Digital	Documento de Texto	Archivo de Gestión de la Gerenteía Delegada para el Medio Ambiente
RELACIONES TÉCNICAS CON EL CONGRESO	Relaciones Técnicas solicitadas o que requiera el Congreso en el ámbito de la CGR	SI	Informes Técnicos al Congreso	Informes Técnicos con temática especifica	Español	Fisico-Digital	Documento de Texto	Archivo de Gestión de la Gerenteía Delegada para el Medio Ambiente
SUPERVISIÓN DE CONTRATOS	Supervisión	SI	Supervisión de Contratos	Supervisión de Contratos	Español	Fisico	Documento de Texto	Archivo de Gestión de la Gerenteía Delegada para el Medio Ambiente

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS **Versión 1.0**

CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
SOLICITUDES DE AJUSTES AL PLAN GENERAL DE AUDITORÍA	Solicitud de	SI	Solicitud de ajuste al Plan General de Auditoria	Solicitud de ajuste al Plan General de Auditoria	Español	Fisico - Electrónico	Documento de Texto	Archivo de Gestión de la Gerenteía Delegada para el Medio Ambiente
CONTROL EXCEPCIONAL	Control Exce	SI	Control Excepcional	Control Excepcional	Español	Fisico-Digital	Documento texto - Digital-SICA	Archivo de Gestión de la Gerenteía Delegada para el Medio Ambiente
URGENCIA MANIFIESTA	Urgencia Mani	SI	Urgencia Manifiesta	Urgencia Manifiesta	Español	Fisico-Electrónico	Documento de Texto	Archivo de Gestión de la Gerenteía Delegada para el Medio Ambiente
ACTAS (ACTAS DE SEGUIMIENTO AL PLAN GENERAL DE AUDITORIA - PGA	Actas de segui	SI	Actas de seguimiento al Plan General de Auditoria -PGA	Actas de seguimiento al Plan General de Auditoria - PGA	Español	Fisico-Digital	Documento texto - Digital	Documento texto - Digital
ACTUACIONES ESPECIALES DE CONTROL FISCAL	Informes	SI	Actuaciones especiales de control fiscal	Informes de Auditoria con tematica especifica: Gestión Fiscal, de seguimiento, de Observatorios, de consultas de información, de fiscalización entre	Español	Fisico-Digital	Documento texto - Digital-SICA	Archivo de Gestión de la Gerenteía Delegada para el Medio Ambiente
AUDITORÍA	Auditorias	SI	Auditorias	Auditorias. Los Informes de Apoyo Técnico, Austeridad del gasto, de consolidación del control interno	Español	Fisico-Digital	Documento Texto - Digital-SICA	Archivo de Gestión de la Gerenteía Delegada para el Medio Ambiente
BENEFICIOS DEL PROCESO AUDITOR	Informes	SI	Beneficios del proceso auditor	Beneficios del proceso auditor	Español	Fisico-Digital	Documento texto - Digital-SICA	Archivo de Gestión de la Gerenteía Delegada para el Medio Ambiente
INDAGACIONES PRELIMINARES	Indagaciones	SI	Indagación preliminar	Indagación preliminar	Español	Físico	Documento de Texto	Archivo de Gestión de la Gerenteía Delegada para el Medio Ambiente
REPORTES DE OBSERVATORIO (Documentos Electrónicos)	Reportes	SI	Reportes SICA	Asignación de trabajo, Actas de visita Fiscal, Comunicaciones y respuestas de las entidades a observaciones, Papeles de trabajo,Informe definitivo, Informe de muestreo, Informes técnicos	Español	Físico, electrónico - SICA	Físico, electrónico - SICA	Archivo de Gestión de la Gerenteía Delegada para el Medio Ambiente
TRASLADO DE HALLAZGOS FISCALES, DISCIPLINARIOS Y PENALES	Traslado de	SI	Traslado de Hallazgos Fiscales, Penales y Disciplinarios	Traslado de Hallazgos Fiscales, Penales y Disciplinarios	Español	Fisico - Electrónico	Documento de Texto-Digital	Archivo de Gestión de la Gerenteía Delegada para el Medio Ambiente
ACTAS DE ENTREGA DE DEPENDENCIA	Actas de entr	Actas de entrega de dependen	Actas de entrega de dependencia	Actas de entrega de dependencia	Español	Documento texto - Digital	Documento texto - Digital	Archivo de Gestión de la Gerenteía Delegada para el Medio Ambiente
ACTUACIONES ESPECIALES DE CONTROL FISCAL	Actuaciones	Actuaciones Especiales	Actuaciones Especiales de Control Fiscal	Actuaciones Especiales de Control Fiscal	Español	Documento texto - Digital	Documento texto - Digital	Archivo de Gestión de la Gerenteía Delegada para el Medio Ambiente
APOYO AL PROCESO AUDITOR - DIAGNOSTICOS SECTORIALES	Apoyo al proc	Apoyo al proceso auditor - diagnósticos sectoriales	Apoyo al proceso auditor - diagnósticos sectoriales	Apoyo al proceso auditor - diagnósticos sectoriales	Español	Documento texto - Digital	Documento texto - Digital	Archivo de Gestión de la Gerenteía Delegada para el Medio Ambiente
ESTUDIOS E INVESTIGACIONES	Estudios e investigaciones (Análisis sectorial y politicas públicas, Análisis de proyectos de Ley,Publicaciones en revistas, en	Estudios e investigaciones (Análisis sectorial y politicas públicas, Análisis de proyectos de Ley, Publicaciones en revistas, en articulos, e instituciones)	Estudios e investigaciones (Análisis sectorial y politicas públicas, Análisis de proyectos de Ley, Publicaciones en revistas, en articulos, e instituciones)	Estudios e investigaciones (Análisis sectorial y politicas públicas, Análisis de proyectos de Ley, Publicaciones en revistas, en articulos, e instituciones)	Español	Documento texto - Digital	Documento texto - Digital	Archivo de Gestión de la Gerenteía Delegada para el Medio Ambiente

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS								Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
INFORMES	Informes: (Sectoriales al Congreso sobre Estado de los recur	Informes: (Sectoriales al Congreso sobre Estado de los recursos naturales y medio ambiente, Apoyo Técnico, de Gestión	Informes: (Sectoriales al Congreso sobre Estado de los recursos naturales y medio ambiente,Apoyo Técnico, de Gestión, Información Estrategica, Evaluación y Calificación del Sistema de Control Interno, Seguimiento a los Planes de Desarrollo)	Informes: (Sectoriales al Congreso sobre Estado de los recursos naturales y medio ambiente, Apoyo Técnico, de Gestión, Información Estrategica, Evaluación y Calificación del Sistema de Control Interno, Seguimiento a los Planes de Desarrollo)	Español	Documento texto - Digital	Documento texto - Digital	Archivo de Gestión de la Gerenteía Delegada para el Medio Ambiente
ACTAS (COMITÉ DE EVALUACION SECTORIAL, COMITÉ TÉCNICO)	Actas de comi	Actas de comité técnico	Actas de comité técnico	Documento que contiene las conclusiones de la reunión realizada	Español	Físico	Documento de texto	Información pública
ACTUACIONES ESPECIALES DE CONTROL FISCAL	Informe de	Informe final actuación	Informe final actuación especial de fiscalización	Documento que recoge los resultados y pronunciamientos de la actuación especial de fiscalización	Español	Físico / Electrónico	Documento de texto	Información pública
INFORMES FINALES DE AUDITORIA	Informes	Informe final de auditoria	Informe final de auditoria	Documento que recoge los resultados y pronunciamientos de la Auditoria	Español	Físico / Electrónico	Documento de texto	Información pública
RELACIONES TÉCNICAS CON EL CONGRESO	Comunicacio	Comunicaciones oficiales	Comunicaciones oficiales	Documento de respuesta a las solcitudes del Congreso	Español	Físico	Documento de texto	Información pública
APOYO AL PROCESO AUDITOR - DIAGNOSTICOS SECTORIALES	Diagnósticos	Documento con el diagnóstic	Diagnósticos sectoriales	Documento con el diagnóstico sectorial	Español	Físico	Documento de texto	Información pública
ANALISIS SECTORIAL Y DE POLITICAS PUBLICAS	Informe	Informe final	Análisis sectorial y de políticas públicas	Documento que recoge los resultados y pronunciamientos de la Auditoría sobre el tema evaluado	Español	Físico	Documento de texto	Información pública
SOLICITUDES DE AJUSTES AL PLAN GENERAL DE AUDITORÍA	Solicitud de ajust	Solicitud de ajustes al plan de vigilancia	Solicitud de ajustes al plan de vigilancia y control fiscal	Documento que contiene la solicitud aprobada en Comité Técnico	Español	Físico	Documento de texto	Información pública
URGENCIAS MANIFIESTAS	Resolución	Resolución	Resolución	Documento que contiene desición	Español	Físico	Documento de texto	Información pública
TRASLADO DE HALLAZGOS FISCALES, DISCIPLINARIOS Y PENALES	Oficio remisorio	Comunicación oficial de traslado	Comunicación oficial de traslado con incidencia fiscal, disciplinaria y penal	Documento mediante el cual se traslada a la autoridad competente la información relacionada con el traslado según la posible incidencia determinada en el informe final de auditoria.	Español	Físico	Documento de texto	Información pública
ACTAS (COMITÉ DE EVALUACION SECTORIAL, COMITÉ TÉCNICO)	NO	NO	Actas (comité de evaluación sectorial, comité técnico)	No aplica	Español	Físico y electrónico	Papel y documento electrónico	Archivo de Gestión de la Gerenteía Delegada para el Sector Defensa, Justicia y Seguridad
ACTUACIONES ESPECIALES DE CONTROL FISCAL	SÍ	SÍ	Actuaciones especiales de control fiscal	No aplica	Español	Físico y electrónico	Papel y documento electrónico	Archivo de Gestión de la Gerenteía Delegada para el Sector Defensa, Justicia y Seguridad
CONTROL EXCEPCIONAL	SÍ	SÍ	Control excepcional	Control excepcional	Español	Físico y electrónico	Papel y documento electrónico	Archivo de Gestión de la Gerenteía Delegada para el Sector Defensa, Justicia y Seguridad
INDAGACIONES PRELIMINARES	NO	NO	Indagaciones Preliminares	No aplica	Español	Físico y electrónico	Papel y documento electrónico	Archivo de Gestión de la Gerenteía Delegada para el Sector Defensa, Justicia y Seguridad
INFORMES (Auditoria, congreso)	SÍ	SÍ	Informes (Auditoria, congreso)	Informes	Español	Físico y electrónico	Papel y documento electrónico	Archivo de Gestión de la Gerenteía Delegada para el Sector Defensa, Justicia y Seguridad
PROCESOS (Administrativos sancionatorios)	NO	NO	Procesos (Administrativos sancionatorios)	Procesos (Administrativos sancionatorios)	Español	Físico y electrónico	Papel y documento electrónico	Archivo de Gestión de la Gerenteía Delegada para el Sector Defensa, Justicia y Seguridad

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS								Versión 1.0
CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
AUDITORIA	SI	Mediante Aplicativo SICA	Auditoría	Un proceso sistemático que evalua, acorde con las normas de auditoría generalmente aceptadas vigentes, la política pública y/o la gestión y los resultados fiscales de los entes objeto de control fiscal y de los planes, programas, proyectos y/o asuntos a auditar, mediante la aplicación de los sistemas de control fiscal o actuaciones especiales de vigilancia y control, para determinar el cumplimiento de los principios de la gestión fiscal, en la prestación de servicios o provisión de bienes	Español	Físico – Electrónico	Papel generalmente carta y oficio. Electronicos (Magneticos) contenidos en CD: Archivos en formato MS excel.xls y PDF.	Archivo de Gestión de la Gerenteía Delegada para el Sector de Minas y Energía - Aplicativo SICA
BENEFICIOS DEL PROCESO AUDITOR	SI	Mediante Aplicativo SIIGEP	Beneficios del proceso auditor	Forma de medir el impacto del proceso auditor; cuantifica o cualifica el valor agregado generado por el ejercicio del control fiscal, bien se trate de acciones evidenciadas, que correspondan al seguimiento de acciones establecidas en planes de mejoramiento o que sean producto de observaciones, hallazgos, pronunciamientos o advertencias efectuados por la CGR y que exista una relación directa entre la acción de mejoramiento y el beneficio	Español	Físico – Electrónico	Papel generalmente carta y oficio. Electronicos (Magneticos) contenidos en CD: Archivos en formato MS excel.xls y PDF.	Archivo de Gestión de la Gerenteía Delegada para el Sector de Minas y Energía - Aplicativo SIRECI
COMUNICACIONES INFORMATIVAS	NO	Se encuentran copias de las comunicaciones enviadas y recibidas por el despacho	Comunicaciones informativas	Son Las comunicaciones oficiales de caracter informativo enviadas y recibidas en soporte papel	Español	Físico – Electrónico	Papel generalmente carta y oficio. Electronicos (Magneticos) contenidos en CD: Archivos en formato MS excel.xls y PDF.	Archivo de Gestión de la Gerenteía Delegada para el Sector de Minas y Energía - Aplicativo SIGEDOC
CONTROL EXCEPCIONAL	NO	NO	Control excepcional	Facultad para ejercer control fiscal posterior sobre cuentas de cualquier entidad territorial	Español	Físico – Electrónico	Papel generalmente carta y oficio. Electronicos (Magneticos) contenidos en CD: Archivos en formato MS excel.xls y PDF.	Archivo de Gestión de la Gerenteía Delegada para el Sector de Minas y Energía - Aplicativo SICA
DOCUMENTOS DE ORIGEN CIUDADANO	SI	Mediante aplicativo SIPAR	Documentos de origen ciudadano	Documentos relacionadas con denuncias, derechos de petición, acciones populares, tutelas y otras solicitudes	Español	Físico – Electrónico	Papel generalmente carta y oficio. Electronicos (Magneticos) contenidos en CD: Archivos en formato MS excel.xls y PDF.	Archivo de Gestión de la Gerenteía Delegada para el Sector de Minas y Energía - Aplicativo SIPAR
INDAGACIONES PRELIMINARES	NO	Mediante aplicativo SIREF	Indagaciones preliminares	Función de investigación o indagación que se requiera, por hechos relacionados contra los intereses patrimoniales del Estado y que comprometan recursos del mismo	Español	Físico – Electrónico	Papel generalmente carta y oficio. Electronicos (Magneticos) contenidos en CD: Archivos en formato MS excel.xls y PDF.	Archivo de Gestión de la Gerenteía Delegada para el Sector de Minas y Energía - Aplicativo SIREF

Anexo A. (Continuación)

REGISTROS DE ACTIVOS DE INFORMACIÓN -INSTITUTO NACIONAL DE MUSEOS **Versión 1.0**

CATEGORÍA DE INFORMACIÓN	REGISTRO PUB	REGISTRO DISPONIBLE PARA SER	NOMBRE O TÍTULO DE LA CATEGORÍA DE INFORMACIÓN	DESCRIPCIÓN DEL CONTENIDO LA CATEGORÍA DE INFORMACIÓN	IDIOMA	MEDIO DE CONSERVACIÓN Y/O SOPORTE	FORMATO	INFORMACIÓN PÚBLICA O DISPONIBLE
INFORMES	SÍ	SÍ	Informes	Informes	Español	Físico y electrónico	Electrónico y papel	Archivo de Gestión de la Gerenteía Delegada para el Sector Defensa, Justicia y Seguridad - Web
MATRIZ DE RIESGO DE SUJETOS DE CONTROL	NO	SÍ	Matriz de riesgo de sujetos de control	Matriz de riesgo de sujetos de control	Español	Físico y electrónico	Electrónico y papel	Archivo de Gestión de la Gerenteía Delegada para el Sector Defensa, Justicia y Seguridad

NOTA: Para la información suministrada en el Registro de Activos de Información y en el Índice de Información Clasificada y Reservada para cada categoría de información, también aplica para las categorías de información o series y subseries documentales establecidas en las Tablas de Retención Documental de las Gerencias Departamentales Colegiadas.

Consolidado por:

Bertha Cecilia Gonzalez Jimenez _____
Directora Oficina de Comunicaciones y Publicaciones

Iván Alfononso Pertuz _____
Director de Imprenta, Archivo y Correspondencia

Fuente: Instituto Museo Nacional

ANEXO B. ENTREVISTAS

DOMINIO 5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. Resultado de las entrevistas aplicadas a las siguientes áreas: Infraestructura y comunicaciones, Seguridad de la información, Sistemas de información, Administración y desarrollo tecnológico, Mesa de ayuda.

Objetivo de la entrevista: Analizar el nivel de apoyo y orientación de la alta dirección con respecto a las reglas de negocio, las regulaciones y leyes vigentes.

Población estadística: 50 funcionarios,
Muestra: 10 funcionarios
Fecha: Agosto del 2016.

Tabla 2. Entrevista Dominio 5. Políticas de seguridad

Enunciado	**R**
¿Usted considera que existen un grupo de políticas completas para la seguridad de la información definidas por la dirección?	
¿Las políticas de seguridad de la información son aprobadas por la dirección?	
¿Están publicadas y comunicadas las políticas de seguridad de la información a todos los funcionarios y usuarios y partes externas?	
¿Las políticas de seguridad son revisadas a intervalos planificados?	
¿Las políticas de seguridad son actualizadas con las normas vigentes?	
¿Se revisan las políticas de seguridad cuándo se producen cambios significativos para garantizar su conveniencia, suficiencia y eficacia continua?	
¿Actualmente existe normativa relativa a la seguridad de los SI?	
¿Existen procedimientos, normas relacionadas a la seguridad del SI?	
¿Existe un roles con responsable de las políticas, normas y procedimientos?	
¿Existe una metodología pedagogía para la comunicación a los usuarios de las normas	
¿Existen controles regularmente documentados para verificar la efectividad de las políticas?	

Fuente: El autor

DOMINIO 6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN. Resultado de entrevistas aplicadas a las siguientes áreas: Infraestructura y comunicaciones, Seguridad de la información, Sistemas de información, Administración y desarrollo tecnológico, Mesa de ayuda.

Entrevista como herramienta de medición con base a los siguientes objetivos:
Objetivo de la entrevista: Identificar si existe un marco de trabajo de la dirección para controlar la implementación y funcionamiento al interior del instituto.

Población estadística: 50 funcionarios
Muestra: 10 funcionarios.
Fecha: Agosto del 2016.

Tabla 3. Entrevista Dominio 6. Aspectos organizativos de la seguridad de la información

Enunciado	R
¿Existen roles y responsabilidades definidos para las personas implicadas en la seguridad?	
¿Existe responsable encargado de evaluar la adquisición y cambios de SI?	
¿La Gerencia y las áreas administrativas de la Organización participan en los temas de seguridad de la información?	
¿Existen actualmente condiciones contractuales de seguridad con terceros y outsourcing?	
¿Existen criterios definidos para la seguridad en el manejo con terceros?	
¿Existen programas de formación y capacitación en seguridad para los funcionarios, usuarios internos y externos, terceros?	
¿Existen acuerdos de confidencialidad de la información que se acede?	
¿Se revisa la organización de la seguridad periódicamente por una empresa externa?	
¿Existen roles y responsabilidades definidos para las personas implicadas en la seguridad?	
Existe un responsable encargado de evaluar la adquisición y cambios de Sistema de información?	

Fuente: El autor

DOMINIO 7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS. Resultado de las entrevistas aplicadas a las siguientes áreas: Infraestructura y comunicaciones, Seguridad de la información, Sistemas de información, Administración y desarrollo tecnológico.

La siguiente entrevista se aplicó como herramienta de medición con base a los siguientes objetivos:

Objetivo de la entrevista: Analizar el nivel de aseguramiento con que los empleados y contratistas comprenden sus responsabilidades y determinar si son aptos para los roles los cuales fueron previamente considerados.
Población estadística: 50funcionarios, Muestra: 10 funcionarios.
Fecha: Agosto del 2016.

Tabla 4. Entrevista Dominio 7. Seguridad ligada a los recursos humanos

Enunciado	R
¿Se verifican los antecedentes judiciales en cada uno de los candidatos al empleo de acuerdo con las leyes vigentes, regulaciones y normas y en proporción a los requisitos del negocio, la clasificación de la información y los riegos percibidos?	
¿Existen acuerdos contractuales con los empleados y contratistas en donde se indique sus responsabilidades y las de la organización en cuanto a seguridad de la información?	
¿La alta dirección solicita a todos los empleados y contratistas que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por el instituto?	
¿Los funcionarios del instituto reciben información adecuada en concientización y actualizaciones regulares en las políticas y procedimientos establecidos?	
¿Existe un proceso disciplinario formal y sabido por los funcionarios para tomar acciones en contra de los empleados que hayan cometido una infracción a la seguridad y privacidad de la información?	
¿Existe comunicación de las responsabilidades y funciones de la seguridad de la información que siguen en vigor después de la desvinculación o cambio de la relación laboral?	

Fuente: El autor

DOMINIO 8. GESTIÓN DE ACTIVOS. Resultado de las entrevistas aplicadas a las siguientes áreas: Infraestructura y comunicaciones, Seguridad de la información, Sistemas de información, Administración y desarrollo tecnológico.

Entrevista como herramienta de medición con base a los siguientes objetivos:

Objetivo de la entrevista: Determinar la seguridad en los activos del instituto, las responsabilidades de protección pertinentes.

Población: 50 funcionarios
Muestra: 10 funcionarios.
Fecha: Agosto del 2016.

Tabla 5. Entrevista Dominio 8. Gestión de activos

Enunciado	R
¿Existen un inventario de activos de información actualizado?	
¿El Inventario contiene activos de datos, software, equipos y servicios?	
¿Se dispone de una clasificación de la información según la criticidad de la misma?	
¿En la actualidad existe un responsable de los activos?	
¿Existen procedimientos para clasificar la información?	
¿Existen procedimientos de etiquetado y rotulado de la información?	
¿Los activos que se mantienen en inventario pertenecen a un dueño?	
¿Al finalizar el contrato laboral todos los funcionarios y usuarios de terceras partes devuelven todos los activos que pertenecen al instituto?	
¿Se implementan procedimientos para gestión de medios removibles?	
¿Se eliminan los medios de forma segura cuando no se necesitan más?	
¿Se protegen contra acceso no autorizado todos los medios que contienen información para uso inadecuado o corrupción durante el trasporte?	

Fuente: El autor

DOMINIO 9. CONTROL DE ACCESOS. La entrevista se aplicó a funcionarios de las oficinas de tecnología de la información.
Entrevista oficina de tecnología de la información y las comunicaciones.

Objetivo de la entrevista: Analizar cómo está el acceso a los sistemas de información, bases de datos y servicios de información en el instituto.

Población: 50 funcionarios
Muestra: 10 funcionarios.
Fecha: Agosto del 2016.

Tabla 6. Entrevista Dominio 9. Control de acceso

Enunciado	R
¿Los sistemas operativos de los servidores se parchan con frecuencia?	
¿El nivel de seguridad poseen los protocolos para establecer conexiones a los usuarios son considerables?	
¿Se realizan hacking ético, pent testing, con regularidad en el IMN?	
¿El nivel de las contraseñas de acceso a los diferentes aplicativos en producción es alto?	
¿Usted posee conocimientos acerca de la seguridad de la información?	
¿El Nivel de seguridad de la información que usted considera que posee el instituto es considerable?	
¿El nivel en que se encuentran los controles de riesgos de seguridad es alto o considerable?	
¿Con frecuencias se hacen revisiones periódicas para incluir cambios a los roles?	
¿Se exige el uso de las buenas prácticas de seguridad en la información confidencial para la autenticación?	
¿El grado tecnológico con que cuenta el instituto a nivel de seguridad es bueno?	

Fuente: El autor

DOMINIO 10. CRIPTOGRAFÍA. La entrevista de aplico a funcionarios de las áreas de: Infraestructura y comunicaciones, Seguridad de la información, Sistemas de información, Administración y desarrollo tecnológico.

Objetivo de la entrevista: Analizar el uso de sistemas y herramientas técnicas criptográficas para la protección de la información en el instituto.

Población: 50 funcionarios
Muestra: 10 funcionarios.
Fecha: Agosto del 2016.

Tabla 7. Entrevista Dominio 10. Criptografía

Enunciado	R
¿Usted conoce las políticas de los controles criptográficos?	
¿Se desarrolla o implementa una política sobre el uso, protección y ciclo de vida de las claves criptográficas a través de todo su ciclo?	
¿Las credenciales de acceso caducan cada 30 días?	
¿Se realizan seguimientos y auditorias relacionadas con las gestiones de claves criptográficas?	
¿Las claves criptográficas son destruidas cuando caducan?	
¿Usted considera que las claves criptográficas de accesos son seguras?	
¿Todas las aplicaciones validan el acceso contra el directorio activo del instituto con claves criptográficas?	
¿Existe un único servidor de autenticación a las diferentes aplicaciones?	
¿Las firmas digitales son validadas con una organización externa?	
¿Existe en algunas bases de datos contraseñas o datos confidenciales almacenados de forma plana?	
¿Los niveles de entropías en las credenciales son altas?	
¿Utiliza usted dispositivos móviles para realizar trasmites con identificación y/o firmas electrónicas?	

Fuente: El autor

DOMINIO 11. SEGURIDAD FÍSICA Y AMBIENTAL. La entrevista de aplico a funcionarios de las áreas de: Infraestructura y comunicaciones, Seguridad de la información.

Objetivo de la entrevista: Analizar el nivel de seguridad con el uso adecuado y eficaz de los controles a los accesos físicos no autorizados, daños e interferencia contra las instalaciones de procesamiento de la información.

Población: 50 funcionarios
Muestra: 10 funcionarios
Fecha: Agosto del 2016

Tabla 8. Entrevista Dominio 11. Seguridad física y ambiental

Enunciado	R
¿El Datacenter se encuentra resguardado del acceso exterior?	
¿Existe un centro de datos con todas las normas de seguridad?	
¿Existe personal de vigilancia en el instituto?	
¿Las horas laborales extras al trabajo cotidiano son auditadas?	
¿En el instituto se utilizan controles de accesos físicos?	
¿El edificio posees salidas de emergencias señalizadas?	
¿El área de almacén es suficiente para guardar todos los suministros?	
¿NO existen materiales inflamables dentro del área de TI?	
¿Existe oficina externa al instituto donde llegue la correspondencia?	
¿Existen barreras físicas que aíslen áreas coyunturales del instituto?	
¿Se utilizan circuitos cerrados de televisión en las áreas comunes?	
¿Existe un control de activos de entrada y salida en IMN?	
¿El estado de las canaletas y cableados eléctricos son buenos?	
¿Existe un Firewall en el instituto y se entiende para que debe existir?	
¿En la entidad NO hay equipos de cómputos en el piso?	
¿NO se utilizan aire acondicionados en el Datacenter?	
¿Hay reguladores y UPS en todos los equipos de cómputo?	
¿Existe planta eléctrica para la generación en caso de emergencia?	

Fuente: El autor

DOMINIO 12. GESTIÓN DE OPERACIONES. La entrevista de aplico a funcionarios de las áreas de: Infraestructura y comunicaciones, Seguridad de la información.

Objetivo de la entrevista: Analizar los controles y procedimientos de las operaciones, el desarrollo y mantenimiento con su respectiva documentación actualizada en la OTI.

Población: 50 funcionarios
Muestra: 10 funcionarios
Fecha: Agosto del 2016.

Tabla 9. Dominio 12. Resultado de entrevista de gestión de operaciones

Enunciado	R
¿Los procedimientos operativos se encuentran documentado?	
¿Se controlan los cambios que afectan la seguridad de la información en la organización y procesos internos, instalaciones procesamientos de información?	
¿Se monitorea los recursos con proyecciones de requisitos de capacidad?	
¿Los ambientes de desarrollo, pruebas, capacitación y producción están por separados?	
¿Existe un software versionador estándar y centralizado para todos los grupos de desarrollo?	
¿Periódicamente se implementan controles para la detección y prevención y recuperación antes afectaciones de Malware?	
¿A las copias de seguridad y archivos sensibles se aplica técnica de cifrado?	
¿Se realizan registros de fallas y operadores para garantizar la identificación de los problemas de SI?	
¿Se implementan procedimientos para controlar la instalación de software en sistemas operacionales?	
¿Se realiza informes de vulnerabilidades a los responsables involucrados?	
¿Las reglas que rigen la instalación de software son establecidas para su implementación?	
¿Los procedimientos y requerimientos responsables de auditorías son documentados?	

Fuente: El autor

DOMINIO 13. SEGURIDAD EN LAS COMUNICACIONES. La entrevista de aplico a funcionarios de las áreas de: Infraestructura y comunicaciones, Seguridad de la información.

Análisis de resultados de las entrevistas realizadas seguidamente aplicadas las diferentes entrevistas a las oficinas y dependencias del IMN. Se prosiguió con el respectivo análisis determinando la tendencia de los resultados de cada pregunta.

Objetivo de la entrevista: determinar cómo se encuentra la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte.

Población: 50 funcionarios
Muestra: 10 funcionarios
Fecha: Agosto del 2016.

Tabla 10. Entrevista Dominio 13. Seguridad en las comunicaciones

Enunciado	R
¿Se administran y controlan las redes para proteger la información en sistemas y aplicaciones?	
¿Se identifican e incluyen en los acuerdos de servicios (CLA), los mecanismos de seguridad, niveles de servicios y requisitos para administrar servicios de red?	
¿Las redes son desagregadas en función de los grupos de servicios, usuarios y sistemas de información?	
¿Existen políticas y procedimientos de intercambio de información?	
¿En la mensajería electrónica se protege adecuadamente la información?	
¿Ha firmado un acuerdo de confidencialidad diferente al del contrato laboral?	
¿Están definidas las responsabilidades y los procedimientos para el tratamiento de los eventos y debilidades de la seguridad de la información?	
¿Usted considera se realiza un proceso de mejora continua al monitoreo, evaluación, y gestión de incidentes de seguridad de la información?	
¿Cuándo se halla evidencia, esta se recolecta y documenta para garantizar el cumplimiento de los requisitos legales?	
¿Se realizan copias de seguridad a los activos de información programadas?	

Fuente: El autor

DOMINIO14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS. La entrevista de aplico a funcionarios de las áreas de: Infraestructura y comunicaciones, Seguridad de la información.

Objetivo de la entrevista: Analizar y determinar el nivel de aseguramiento de los sistemas de información en todo el ciclo, incluyendo los requisitos para los sistemas de información que proporcionan servicios en las redes públicas.

Población: 50 funcionarios
Muestra: 10 funcionarios
Fecha: Agosto del 2016.

Tabla 11. Entrevista Dominio 14. Adquisición, desarrollo y mantenimiento de sistemas

Enunciado	R
¿Usted considera que los ambientes de desarrollo son seguros?	
¿Existe un marco de seguridad o framework de referencia para el desarrollo seguro de aplicaciones?	
¿Se utiliza una metodología o técnicas para las buenas prácticas de desarrollo de aplicaciones?	
¿Existen políticas que garanticen los ambientes de desarrollos y pruebas que soporten la efectividad y eficiencia?	
¿Se realiza la documentación de cada una de las fases gestionadas en cada uno de los proyecto?	
¿En la actualidad la evaluación del riesgo TI está integrada con la evaluación del riesgo del instituto?	
¿Existe algún procedimiento o mecanismo para la gestión de cambios o requerimientos durante el desarrollo, compra o adquisición de aplicativos?	
¿Se generan acciones preventivas y correctivas después de los análisis de vulnerabilidades y posibles amenazas o riesgos?	
¿Se realizan pruebas de funcionalidad en aspectos de seguridad durante las etapas del desarrollo?	
¿Los datos de las bases de los aplicativos en ambientes de pruebas, ambientes desarrollo o de capacitación son datos ficticios?	

Fuente: El autor

DOMINIO 15. RELACIÓN CON PROVEEDORES. La entrevista de aplico a los funcionarios de las áreas de: Infraestructura y comunicaciones, Seguridad de la información, Mesa de ayuda.

Objetivo de la entrevista: Determinar el nivel de protección en seguridad de los activos del instituto a los que tienen acceso los proveedores. Analizar la seguridad de la información en las relaciones con los proveedores.

Población: 50 funcionarios
Muestra: 10 funcionarios
Fecha: Agosto del 2016

Tabla 12. Entrevista Domino 15. Relación con proveedores

Enunciado	R
¿Los requisitos de seguridad de la información para mitigar los riegos asociados al acceso de proveedor a los activos de la organización se acuerdan y documentan junto con el proveedor?	
¿Todos los requisitos de Seguridad de la información son definidos y acordados con cada proveedor que acceda, procese, almacene, comunique o proporcione componentes de infraestructura de TI?	
¿Los acuerdos con los proveedores incluyen los requisitos para abordar los riesgos de seguridad de la información asociados a los servicios de TI y las comunicaciones y cadena de suministro?	
¿El instituto supervisa, revisa y audita la entrega de los servicios del proveedor?	
¿Se gestionan los cambios al suministro de los servicios por parte de los proveedores donde se incluya el mantenimiento y la mejora de las políticas de seguridad de la información existente, procedimientos y controles?	
¿Se analiza el nivel de criticidad de la información del negocio, los sistemas y los procesos involucrados y la reevaluación de los riesgos?	

Fuente: El autor

DOMINIO 16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN. La entrevista se aplicó a funcionarios de las áreas de: Infraestructura y comunicaciones, Seguridad de la información, Sistemas de información, Administración y desarrollo tecnológico, Mesa de ayuda.

Objetivo de la entrevista: Analizar el nivel de aseguramiento con el enfoque consistente y eficaz sobre la gestión de los incidentes de seguridad de la información.

Población: 50 funcionarios
Muestra: 10 funcionarios
Fecha: Agosto del 2016

Tabla 13. Entrevista Dominio 16. Gestión de operaciones

Enunciado	R
¿Se hace el requerimiento que los funcionarios o usuarios que observen cualquier debilidad en la seguridad de la información en los sistemas o servicios puedan reportar los incidentes o sospecha?	
¿Se comunican internamente las debilidades de seguridad?	
¿Existe definidas las responsabilidades antes un incidente?	
¿Existe un procedimiento formal de respuesta?	
¿Se comunican o informan con anterioridad los eventos de seguridad mediante los canales de gestión apropiados?	
¿Se establecen responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y metodológica a los incidentes de seguridad de la información?	
¿El instituto define y aplica los procedimientos para la identificación, recolección, adquisición y conservación de información, que pueda servir de evidencia?	
¿Se aplica el conocimiento adquirido al analizar y resolver incidentes de seguridad de la información para mitigar su probabilidad de materialización?	
¿Los incidentes de seguridad de la información son atendidos de acuerdo a los procedimientos documentados?	

Fuente: El autor

DOMINIO 17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO. La entrevista se aplicó a funcionarios de las áreas de: Infraestructura y comunicaciones, Seguridad de la información, Sistemas de información, Administración y desarrollo tecnológico, Mesa de ayuda.

Objetivo de la entrevista: Analizar si se incorpora los aspectos de seguridad de la información con la gestión de la continuidad del negocio en el instituto.
Determinar el nivel de disponibilidad de las instalaciones de procesamiento de la información.

Población: 50 funcionarios
Muestra: 10 funcionarios
Fecha: Agosto del 2016

Tabla 14. Entrevista Dominio 17. Aspectos de seguridad de la información de la gestión de la continuidad del negocio

Enunciado	R
¿Existen procesos para la gestión de la continuidad?	
¿Existe un plan de continuidad del negocio y análisis de impacto?	
¿Existe un diseño, redacción e implantación de planes de continuidad?	
¿Existe un marco de planificación para la continuidad del negocio?	
¿Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio?	
¿Existen procesos para la gestión de la continuidad?	
¿Existe un plan de continuidad del negocio y análisis de impacto?	
¿Existe un diseño, redacción e implantación de planes de continuidad?	
¿Se verifica de manera periódica, los controles de continuidad de la seguridad de la información definida e implementada?	
¿Las instalaciones de procesamientos son implementadas con la redundancia suficiente para cumplir con los requisitos de disponibilidad?	

Fuente: El autor

DOMINIO 18. CUMPLIMIENTO. La entrevista se aplicó a funcionarios de las áreas de: Infraestructura y comunicaciones, Seguridad de la información, Sistemas de información, Administración y desarrollo tecnológico, Mesa de ayuda.

Objetivo de la entrevista: Analizar los cumplimientos con los requisitos legales y contractuales con referencia a la seguridad de la información y todos los requisitos de seguridad. Determinar el aseguramiento y disponibilidad de las instalaciones de procesamiento de la información.

Población: 50 funcionarios
Muestra: 10 funcionarios
Fecha: Agosto del 2016

Tabla 15. Entrevista Dominio 18. Cumplimiento

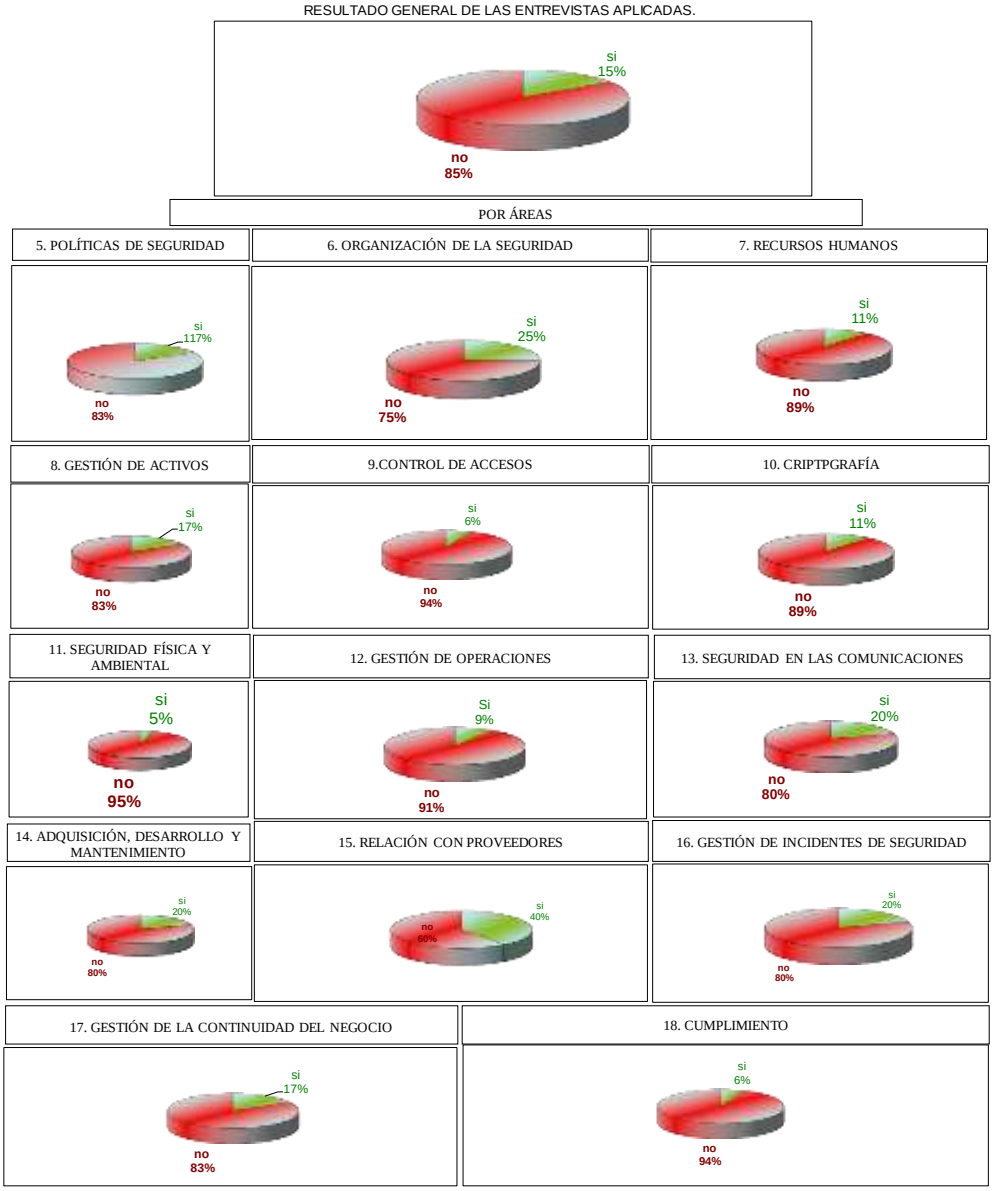
Enunciado	R
¿Se tiene en cuenta el nivel de cumplimiento con la legislación vigente por parte de los sistemas de información en el instituto?	
¿Existe el resguardo de la propiedad intelectual, derechos de autor en los desarrollos de aplicaciones y soluciones propios del instituto?	
¿Existe el resguardo de los registros de la organización?	
¿Existe una revisión general y periódica de la política de seguridad y de la conformidad técnica en el instituto?	
¿Existen consideraciones sobre las auditorías de los sistemas?	
¿Se tiene en cuenta el cumplimiento con la legislación por los sistemas?	
¿Existe el resguardo de la propiedad intelectual?	
¿Los requisitos estatutarios, regulatorios y contractuales están definidos y documentados explícitamente para cada sistema de información?	
¿Los registros se protegen contra pérdida, destrucción, falsificación, acceso sin autorización y emisión sin autorización?	
¿Se asegura la privacidad y protección de la información de identificación personal, como se exige en la legislación y regulaciones pertinentes a Colombia?	
¿Se utilizan controles criptográficos que cumplan con los acuerdos, leyes, y regulaciones pertinentes?	

Fuente: El autor

ANÁLISIS DE RESULTADOS: EN ESTA FASE SE REALIZARON LAS SIGUIENTES ACTIVIDADES:

ENTREVISTA PARA IDENTIFICAR EL ESTADO ACTUAL. Actualmente en el Instituto no se lleva a cabo el 85 % de los controles de la ISO 2700:2013 como se evidencia en los resultados de las entrevistas aplicadas a los funcionarios que pertenecen a las cinco (5) áreas del proceso de tecnología de la información.

Gráficas de tortas como el resumen de resultados de las entrevistas



Fuente: El autor